Prof. Dr. Tobias Singelnstein
Massenbergstraße 11
44787 Bochum

An das
Bundesverfassungsgericht
Schlossbezirk
76131 Karlsruhe

Bochum, 02. Juli 2019

Verfassungsbeschwerde

1. der Frau Silvia Gingold
2. des Herrn Norbert Birkwald
3. der Frau Rechtsanwältin Seda Basay-Yildiz
4. des Herrn Rechtsanwalts Tronje Dröhmer
5. des Herrn Franz Josef Hanke
6. des Herrn Klaus Landefeld
7. der Trasec GmbH

gegen

§§ 6 Satz 5, 8 Abs. 4, , 9 Abs. 1, 10 Abs. 2 Nr. 1, 11 Abs. 9, 12 Abs.1, 13, 16, 18 Abs. 3,
20 Abs. 1 Nr. 1 und 2, Abs. 2 Satz 1 Nr. 2, Abs. 2 Satz 3,
21 Abs. 2, 26 Abs. 1 Hessisches Verfassungsschutzgesetz (HVSG)
§§ 15 b, 15c, 25a Hessisches Sicherheits- und Ordnungsgesetz (HSOG),
in der Fassung des Gesetzes zur Neuausrichtung des Verfassungsschutzes in Hessen vom 25. Juni 2018, veröffentlicht am 03. Juli 2018 im Gesetz- und Verordnungsblatt für das Land Hessen, 13. Ausgabe, S. 302.

Namens und in Vollmacht der Beschwerdeführerinnen und Beschwerdeführer erhebe ich Verfassungsbeschwerde. Ich rüge Verletzungen von Art. 1 Abs. 1, Art. 2 Abs. 1, Art. 10 Abs. 1, Art. 13 Abs. 1, Art. 19 Abs. 4 GG.

Gliederung des Schriftsatzes

A. ZUSAMMENFASSUNG ... 5

B. SACHVERHALT ... 7

I. Die angegriffenen Regelungen im HVSG ... 7

II. Die angegriffenen Regelungen im HSOG ... 8

III. Die Beschwerdeführer*innen ... 14

1. Beschwerdeführerin zu 1 ... 14
2. Beschwerdeführer zu 2 ... 16
3. Beschwerdeführerin zu 3 ... 17
4. Beschwerdeführer zu 4 ... 18
5. Beschwerdeführer zu 5 ... 19
6. Beschwerdeführer zu 6 ... 21
7. Beschwerdeführerin zu 7 ... 22

C. ZULÄSSIGKEIT ... 22

I. Frist ... 22

II. Beschwerdefähigkeit ... 23

1. Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme . 24
2. Anwendbarkeit auf die Beschwerdeführerin zu 7 ... 24

III. Beschwerdebefugnis ... 25

1. Beschwerdebefugnis der Beschwerdeführer*innen zu 1-5 in Bezug auf die gerügten Neuregelungen im HVSG und § 25a HSOG ... 25
   a) Grundrechtsrügen ... 25
   b) Eigene und gegenwärtige Beschwer ... 26
      (1) In Bezug auf die angegriffenen Regelungen im HVSG ... 26
      (2) In Bezug auf die automatisierte Datenanalyse, § 25a HSOG ... 28
   c) Unmittelbare Beschwer ... 31
2. Beschwerdebefugnis der Beschwerdeführer*innen 1-7 in Bezug auf die Quellen-TKÜ und Online-Durchsuchung in §§ 15b, 15c HSOG ... 31
   a) Herausgehobene Rolle von Schwachstellen-Exploits bei der Umsetzung von Quellen-TKÜ ... 32
   b) Schutzdimension des IT-Grundrechts ... 33

c) Aufgabe des Landes Hessen bei der Gewährleistung der IT-Sicherheit 33
d) Besondere Schutzbedürftigkeit der Beschwerdeführer*innen 1-7 34
e) Eigene, gegenwärtige und unmittelbare Betroffenheit 37

IV. Subsidiarität der Verfassungsbeschwerde 37

D. BEGRÜNDETHEIT 40

I. Grundrechtswidrigkeit der angegriffenen Regelungen im HVSG 40
1. Grundrechtswidrigkeit der angegriffenen Überwachungsermächtigungen 40
a) Verfassungsrechtliche Maßstäbe 40
b) Ortung von Mobilfunkendgeräten, § 9 Abs.1 HVSG 43
c) besondere Auskunftsersuchen, § 10 Abs. 2 Satz 1 Nr. 1 HVSG 46
d) Einsatz von verdeckten Mitarbeiter*innen und Vertrauensleuten, §§ 12, 13 HVSG 47
(1) Einstufung als schwerwiegender Grundrechtseingriff 47
(2) Unzureichende Eingriffsschwelle 49
2. Verfahrensanforderungen 51
a) Unzureichende Benachrichtigungspflichten 51
b) Auskunftsrechte gemäß § 26 HVSG 54
3. Datenverarbeitung und Datenübermittlung 56
a) Unzureichende Beschränkung der Datenverarbeitung aus Wohnraumüberwachung und Zugriffen auf informationstechnische Systeme, §§ 16, 18 Abs. 3 HVSG 56
b) Informationsübermittlung durch das Landesamt innerhalb des öffentlichen Bereichs gemäß § 20 Abs.1 und Abs. 2 HVSG 58
(1) Verfassungsrechtliche Anforderungen 59
(2) Sonderregelung für Übermittlungen an besondere Vollzugsbehörden, § 20 Abs. 2 Satz 1 Nr. 2 HVSG 59
(3) Informationsübermittlung wegen Staatsschutzdelikten, § 20 Abs. 2 Satz 3 HVSG 61
(4) Allgemeine Übermittlungsermächtigung, § 20 Abs. 1 HVSG 62
(5) Auslandsübermittlungen, § 21 Abs. 2 HVSG 63

II. Verfassungswidrigkeit der angegriffenen Regelungen im HSOG 64
1. Online-Durchsuchung und Quellen TKÜ, §§ 15b, 15c HSOG 64
a) objektivrechtliche Anforderungen des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme 65
b) Aufgabe des Landes Hessen bei der Gewährleistung der IT-Sicherheit 67
c) Anwendbarkeit auf juristische Personen 70
2. Anwendung zur automatisierten Datenanalyse, § 25a HSOG 70
a) Verfassungsrechtliche Maßstäbe 70

b) Grundrechtswidrigkeit der automatisierten Anwendung zur Datenanalyse nach § 25a HSOG 73
(1) Intensität des Eingriffs 73
(2) Eingriffsschwelle nicht hinreichend qualifiziert 76
(3) Verfahrenssicherungen 80

A. Zusammenfassung

Die Verfassungsbeschwerde richtet sich gegen Neuregelungen des Hessischen Verfassungsschutzgesetzes (im Folgenden: HVSG) sowie des Hessischen Sicherheits- und Ordnungsgesetzes (im Folgenden: HSOG), die am 4. Juli 2018 durch das Gesetz zur Neuausrichtung des Verfassungsschutzes in Hessen in Kraft getreten sind.

Die Verfassungsbeschwerde rügt einzelne, neu geregelte Überwachungsermächtigungen im HVSG, namentlich die Ermächtigungen zur Ortung von Mobilfunkendgeräten (§ 9 Abs. 1 HVSG), zum Einsatz von Verdeckten Ermittlern (§12 Abs. 1 HVSG) und Vertrauensleuten (§ 13 HVSG) und Erweiterung des besonderen Auskunftsersuchens auf sämtliche Verkehrsunternehmen (§ 10 Abs. 2 Nr. 1 HVSG). Gegenstand der Beschwerde sind die materiellen Eingriffsschwellen dieser Regelungen, die es dem Landesamt für Verfassungsschutz Hessen (im Folgenden: Landesamt) ermöglichen, Überwachungsmaßnahmen von hoher Eingriffsintensität im Wesentlichen auf allgemeine Erfahrungssätze zu stützen, deren Gebrauch rechtlich nicht näher angeleitet wird. Darüber hinaus richtet sich die Beschwerde gegen unzureichende flankierende Verfahrensvorschriften, insbesondere gegen die restriktiven Benachrichtigungspflichten und Auskunftsrechte Betroffener.

Zudem richtet sich die Beschwerde gegen die fehlende Nutzungsbeschränkung für übermittelte Daten, die aus Wohnraumüberwachungen oder Online-Durchsuchungen stammen. Diesbezüglich weist das Normengefüge der §§ 16, 18 HVSG eine Lücke auf. Gerügt wird auch die erweiterte Informationsübermittlung des Landesamts an inländische öffentliche Stellen in § 20 Abs. 1 Nr. 1 und 2, Abs. 2 Satz 1 Nr. 2, Abs. 2 Satz 3 HVSG und an ausländische öffentliche Stellen in § 21 Abs. 2 HVSG, deren Eingriffsschwelle nicht hinreichend konkret und qualifiziert ist und folglich nicht den Anforderungen an eine Zweckänderung genügt.

Die Beschwerde gegen Neuregelungen im HSOG betrifft die überarbeitete und erweiterte Rechtsgrundlage für „Telekommunikationsüberwachung an informationstechnischen Systemen“ (Quellen-TKÜ) in § 15b HSOG, die in § 15c HSOG neu geschaffene Rechtsgrundlage für den „verdeckten Eingriff in informationstechnische Systeme“ (Online-Durchsuchung) und die neue Rechtsgrundlage in § 25a HSOG zur Nutzung einer automatisierten Anwendung zur Datenanalyse (automatisierte Datenanalyse). Die Quellen-TKÜ und Online-Durchsuchung ermöglichen die Einspeisung eines Staatstrojaners in ein informationstechnisches System (IT-System). Dies führt zu schwerwiegenden, nicht mehr hinnehmbaren Risiken für die Informationssicherheit in der Bundesrepublik. Denn die Rechtsgrundlagen schließen es nicht aus, dass die Polizei Hessen zur Durchführung solcher Überwachungen noch unbekannte Sicherheitslücken von Hard- und Software ausnutzt und geheim hält. Diese Sicherheitslücken können ebenso wie durch die Polizei Hessen auch durch Dritte ausgenutzt werden, was schwere Schäden zur Folge haben kann. Die staatliche Ausnutzung und Geheimhaltung solcher Sicherheitslücken steht darum mit dem Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme in seiner objektiv-rechtlichen Dimension nicht in Einklang.

Die automatisierte Datenanalyse gemäß § 25a HSOG ermöglicht die Zusammenführung und Auswertung großer Mengen personenbezogener Daten mit Hilfe einer Analysesoftware, um „Beziehungen oder Zusammenhänge zwischen Personen, Personengruppierungen, Institutionen, Organisationen, Objekten und Sachen“ herzustellen. Obwohl die Erhebung der einzelnen Datensätze nach anderen Ermächtigungsgrundlagen erfolgt, ist die Zusammenführung und gemeinsame Analyse aufgrund des zusätzlichen Informationsgewinns ein eigener Grundrechts-

eingriff. Durch die komplexen Verarbeitungs- und Verknüpfungsmöglichkeiten gewinnen zuvor möglicherweise belanglose Informationen einen neuen Gehalt. Die Verknüpfung der polizeilichen Datenbanken mit Informationen aus sozialen Medien und anderen öffentlichen und nicht-öffentlichen Quellen ermöglicht einen nahezu lückenlosen Einblick in das Leben, die Beziehungen und Netzwerke betroffener Personen. Auch über unmittelbare Zielpersonen hinaus hat die automatisierte Datenanalyse eine große Streubreite und kann über die Verknüpfung von Ereignissen, Orten, Objekten und Menschen nahezu jede*n Bürger*in als Beifang erfassen.

Derartige Datenverarbeitungsprogramme haben eine neue Qualität und erhöhte Eingriffsintensität im Vergleich zur herkömmlichen Datennutzung. Vor diesem Hintergrund kann die Datenanalyse mit Hilfe komplexer Datenverarbeitungsprogramme nicht als weitere Nutzung klassifiziert und an den Grundsätzen der Zweckbindung gemessen werden, sondern muss sich an den im Urteil des angerufenen Gerichts zur Rasterfahndung entwickelten Grundsätzen messen lassen,

vgl. BVerfGE 115, 320 (362).

Erforderlich ist dementsprechend eine konkrete Gefahr für hochrangige Rechtsgüter. Diesen Anforderungen genügt § 25a HSOG nicht, denn die vorbeugende Straftatenbekämpfung der in § 100a Abs. 2 StPO genannten Straftaten ermöglicht den Einsatz der automatisierten Datenanalyse weit im Vorfeld einer konkreten Gefahr und zum Schutz von Rechtsgütern geringen Gewichts.

B. Sachverhalt

Gegenstand der Verfassungsbeschwerde sind Neuregelungen des HVSG sowie des HSOG, die am 4. Juli 2018 durch das Gesetz zur Neuausrichtung des Verfassungsschutzes in Hessen in Kraft getreten sind. Artikel 1 enthält eine umfängliche Überarbeitung des HVSG, Artikel 3 ergänzt das HSOG um neue Eingriffsermächtigungen.

I. Die angegriffenen Regelungen im HVSG

Artikel 1 des Gesetzes zur Neuausrichtung des Verfassungsschutzes in Hessen enthält eine grundlegende Umgestaltung und Neufassung des HVSG bei gleichzeitiger Aufhebung des bisherigen Gesetzes (§ 29 HVSG). Ziel der Reform ist die Verbesserung der Zusammenarbeit von Nachrichtendiensten, Polizei- und sonstigen Sicherheitsbehörden und die größtmögliche Harmonisierung auf dem Gebiet des Verfassungsschutzes.

vgl. Gesetzesentwurf, LT-Drs. v. 14.11.2017, S. 24.

Die Verfassungsbeschwerde richtet sich gegen einzelne Überwachungsermächtigungen des HVSG einschließlich zugehöriger Verfahrensregelungen zur Gewährleistung von Transparenz und effektiven Rechtsschutz, die Regelung über den datenschutzrechtlichen Auskunftsanspruch des Betroffenen, die Ermächtigung zur Weiterverarbeitung von Daten, sowie mehrere Ermächtigungen zur Übermittlung von Informationen durch das Hessische Landesamt für Verfassungsschutz (im Folgenden: Landesamt) an andere Stellen.

Im Einzelnen richtet sich die Verfassungsbeschwerde gegen
die Ermächtigung zur Ortung von Mobilfunkendgeräten in § 9 Abs. 1 HVSG, der den früheren § 5 Abs. 2 HVSG a.F. ersetzt, sowie § 10 Abs. 2 Nr. 1 HVSG, durch den der zuvor in § 4a HVSG a.F. enthaltene Auskunftsanspruch auf alle Verkehrsunternehmen erstreckt wurde, sowie die Ermächtigungen zum Einsatz von Verdeckten Mitarbeiterinnen und Verdeckten Mitarbeitern und zum Einsatz von Vertrauensleuten, die in §§ 12 Abs. 1, 13 HVSG erstmals eigenständig geregelt wurden. Zudem richtet sich die Beschwerde gegen die teils fehlenden (§§ 9, 12, 13 HVSG) und im übrigen sehr restriktiven (§§ 6 S. 5, 10 Abs. 6, 8 Abs. 4, 11 Abs. 9 HVSG) Benachrichtigungspflichten zur Gewährleistung von Transparenz und effektivem Rechtsschutz, was wiederum zur Unverhältnismäßigkeit der genannten Normen führt und das Recht auf individuellen Rechtsschutz verletzt.

Darüber hinaus rügt die Beschwerde eine im Zusammenspiel zwischen §§ 16, 18 HVSG existierende Lücke für den verfassungskonformen Umgang mit übermittelten Daten aus Wohnraumüberwachung und Online-Durchsuchung.
§ 18 HVSG regelt die Übermittlung von Daten an das Landesamt. Neu ist, dass die in § 18 Abs. 1 HVSG aufgezählten Behörden und sonstigen öffentlichen Stellen des Landes zur Übermittlung von Daten verpflichtet sind, wenn die Daten zur Erfüllung der Aufgaben des Landesamts erforderlich sind. Während in § 18 Abs. 3 HVSG für Daten aus Telekommunikationsüberwachung eine qualifizierte Eingriffsschwelle normiert ist, fehlt es an einer entsprechenden Regelung für Daten aus Wohnraumüberwachung und Online-Durchsuchung. Auch § 16 HVSG, der die Speicherung, Veränderung und Nutzung von Daten durch das Landesamt reguliert, enthält keine Beschränkung für übermittelte Daten aus Wohnraumüberwachung und Online-Durchsuchung und verfehlt in dieser Hinsicht die verfassungsrechtlichen Anforderungen an die Zweckänderung.

Darüber hinaus richtet sich die Beschwerde gegen die Ermächtigung des Landesamts zur Übermittlung von Daten an andere öffentliche Stellen gemäß
§ 20 Abs. 1 Nr. 1 und 2, Abs. 2 Satz 1 Nr. 2, Abs. 2 Satz 3
HVSG. § 20 HVSG strukturiert die Übermittlungsbefugnisse und -pflichten des Landesamts neu. § 20 Abs. 1 verleiht dem Landesamt die Befugnis, Daten an inländische öffentliche Stellen zu übermitteln, ohne dafür qualifizierte Übermittlungsvoraussetzungen zu schaffen. Die Verfassungsbeschwerde greift diese Regelung insoweit an, als davon auch Daten umfasst sind, die mit nachrichtendienstlichen Mitteln erhoben wurden. § 20 Abs. 2 Satz 1 Nr. 2 HVSG enthält einen qualifizierten Übermittlungstatbestand für die Übermittlung an Vollzugsbehörden. Die Verfassungsbeschwerde beschränkt sich insoweit auf die Erstreckung der Übermittlungsbefugnisse auf Daten, die der Empfänger nur zur Verfolgung oder Verhütung von Straftaten von erheblicher Bedeutung bedarf. Insbesondere rügt die Verfassungsbeschwerde die in § 20 Abs. 2 Satz 3 HVSG enthaltene Definition der erfassten Straftaten.
Die Verfassungsbeschwerde richtet sich zudem gegen die Befugnis des Landesamts zur Informationsübermittlung an ausländische staatliche Stellen gemäß § 21 Abs. 2 HVSG.
§ 21 Abs. 2 HVSG ermöglicht die Übermittlung von Daten, die mit nachrichtendienstlichen Mitteln erhoben werden, die Verfassungsbeschwerde richtet sich gegen die sehr weite Übermittlungsschwelle der „Wahrung erheblicher Sicherheitsinteressen“ des Empfängers sowie fehlende verfahrensrechtliche Sicherungen.
Gegenstand der Beschwerde sind zudem Beschränkungen des Auskunftsanspruches gemäß § 26 Abs. 1 HVSG. § 26 HVSG ersetzt den bislang in § 18 HVSG enthaltenen Auskunftsanspruch und führt in § 26 Abs. 1 HVSG das Erfordernis der Darlegung eines Auskunftsinteresses durch den Antragstellenden ein. Darüber hinaus schließt § 26 Abs. 1 HVSG die Auskunft über Herkunft und Empfänger personenbezogener Daten aus und beschränkt den Auskunftsanspruch grundsätzlich auf Daten in strukturierten Dateien.

II. Die angegriffenen Regelungen im HSOG

Die Verfassungsbeschwerde wendet sich gegen die überarbeitete Rechtsgrundlage zur Quellen-TKÜ gemäß § 15b HSOG, sowie gegen die durch § 15c HSOG eingeführte Ermächtigung zur Online-Durchsuchung. Die Ermächtigung zur Quellen-TKÜ ist im Grundsatz bereits am 14. Dezember 2009 im HSOG eingeführt worden,

> Artikel 1 des Gesetzes zur Änderung des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung und anderer Gesetze vom 14. Dezember 2009 (GVBl IS. 635).

Durch Art. 3 des Gesetzes zur Neuausrichtung des Verfassungsschutzes in Hessen ist § 15b HSOG angepasst worden, insbesondere sind die Voraussetzungen der Quellen-TKÜ in § 15 Abs. 1 HSOG erweitert worden. Während in der alten Fassung des § 15b Abs. 1 HSOG die Quellen-TKÜ nur zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person möglich war, enthält § 15b HSOG nunmehr durch den Verweis auf § 15a Abs. 1 HSOG eine Erweiterung auf Gefahren für Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Bundes oder eines Landes oder die Grundlagen der Existenz der Menschen berührt sowie eine Vorverlagerung des Gefahrenbegriffs für die Abwehr terroristischer Gefahren.

§ 15c HSOG ist neu geschaffen worden und ermöglicht den Zugriff auf IT-Systeme und die Auslesung dort gespeicherter persönlicher Daten sowie die Verfolgung von Aktivitäten und Bewegungen der Betroffenen am Computer und im Netz. Sowohl die Quellen-TKÜ als auch die Online-Durchsuchung sind möglich zur Abwehr einer dringenden Gefahr für Leib, Leben oder Freiheit einer Person oder hochrangiger Güter der Allgemeinheit, sowie im Fall der Abwehr terroristischer Gefahren bereits im Vorfeld einer konkreten Gefahr. Insoweit entsprechen §§ 15b, 15c HSOG den Anforderungen des angerufenen Gerichts aus dem Urteil zum BKA-Gesetz.

Die Verfassungsbeschwerde greift diese Regelungen indes nicht aus abwehrrechtlicher Perspektive an, sondern rügt, dass es an gesetzlichen Vorgaben für die Frage fehlt, ob und inwieweit IT-Sicherheitslücken für die Durchführung einer solchen Maßnahme ausgenutzt werden dürfen.

Nach §§ 15b, 15c HSOG soll die hessische Polizei in informationstechnische Systeme eingreifen dürfen, um aus ihnen Daten zu erheben. Hierzu ist es erforderlich, eine hoheitliche Software in das informationstechnische System der von einer Überwachung betroffenen Personen einzuschleusen, die Daten ausliest und an die Polizei übermittelt. Solche Software-Lösungen werden allgemein als Staatstrojaner bezeichnet.

Weder das HSOG in der angegriffenen Fassung noch die Begründung des Gesetzesentwurfs zur Einführung der angegriffenen Normen definieren indes, wie ein Staatstrojaner auf das Zielsystem aufgebracht werden darf. Denkbar sind insbesondere folgende Wege:

- Aufspielen durch Hoheitsträger, etwa bei einer Grenzkontrolle,

- Aufspielen durch Hoheitsträger nach heimlichem Betreten der Räumlichkeiten, in denen sich das System befindet,

- Ausnutzen der Unaufmerksamkeit des berechtigten Nutzers, etwa indem man ihm einen E-Mail-Anhang mit einem (getarnten) Infektions-Programm in der Hoffnung zuspielt, dass er ihn ausführen werde,

- Aufspielen durch Ausnutzen von Sicherheitslücken des genutzten Systems, etwa indem der berechtigte Nutzer zum Aufruf einer speziell präparierten WWW-Seite animiert wird, deren bloße Ansicht aufgrund von Sicherheitslücken zur Infektion des Zielsystems führt (sogenannte *drive by downloads*).

Die Infektion des Zielsystems durch Ausnutzen von Sicherheitslücken bietet für einen Zugriff auf Daten besondere praktische Vorteile. Solche Sicherheitslücken werden deshalb auf dem internationalen Schwarzmarkt für hohe Summen verkauft und spielen eine zentrale Rolle sowohl für Überwachungsmaßnahmen staatlicher Stellen als auch für die organisierte Kriminalität. Es ist davon auszugehen, dass sie auch bei der Umsetzung von Maßnahmen nach §§ 15b, 15c HSOG von herausgehobener Bedeutung sind.

Die Möglichkeit für Polizeibehörden Hessens, Quellen-TKÜ und Online-Durchsuchung durch Ausnutzen von Sicherheitslücken durchzuführen, führt hingegen zu gravierenden Fehlanreizen: Wenn Polizeibehörden solche Lücken ausnutzen dürfen, so haben sie ein – isoliert betrachtet – durchaus nachvollziehbares Interesse daran, ein „Arsenal“ von Sicherheitslücken

aufzubauen, um im Falle des Falles eine Zielperson angreifen zu können. Dieses Interesse wird sie jedoch davon abhalten, eine entdeckte oder gar auf dem Schwarzmarkt angekaufte Sicherheitslücke den jeweiligen Herstellern der IT-Systeme mitzuteilen, damit die Lücken geschlossen werden können. So entstehen Anreize für Behörden, ihnen bekannte Sicherheitslücken gerade nicht schließen zu lassen, sondern sie lieber zu „horten".

Tatsächlich kaufen deutsche staatliche Stellen bereits Sicherheitslücken auf dem Schwarzmarkt auf bzw. haben entsprechende Mittel im Zuge der Haushaltsberatungen bewilligt bekommen. Dies führt dazu, dass Sicherheitslücken nicht nur nicht geschlossen werden. Vielmehr wird der bestehende Schwarzmarkt noch zusätzlich angeheizt. Hohe und steigende Preise für Sicherheitslücken wiederum schaffen vermeidbare Anreize für Sicherheitsforscher, ihre Erkenntnisse nicht den Herstellern zur Verfügung zu stellen, sondern sie auf dem Schwarzmarkt zu verkaufen.

Solange aber die Lücken nicht von den Herstellern der Systeme geschlossen werden können, weil sie von ihnen keine Kenntnis erlangen, können natürlich nicht nur die Polizeibehörden Hessens diese Lücken für den Einsatz von Staatstrojanern ausnutzen. Vielmehr kann jeder, der sie findet oder seinerseits auf dem Schwarzmarkt für Sicherheitslücken kauft, diese Lücken zur Infiltration informationstechnischer Systeme missbrauchen. Das gilt insbesondere auch für Cyber-Kriminelle, die es beispielsweise regelmäßig darauf anlegen, möglichst viele Systeme zum Teil eines sogenannten Botnetzes zu machen oder Zahlungsdaten für Online-Überweisungen von ihnen abzugreifen.

Im Ergebnis setzen staatliche Stellen bereits heute Millionen Nutzer*innen von IT-Systemen weltweit, die von einer den Behörden bekannten Lücke betroffen sind, einem fortbestehenden Risiko von Cyber-Angriffen aus, um diese Sicherheitslücken im Einzelfall selbst für Ermittlungsmaßnahmen in der hier angegriffenen Form ausnutzen zu können. Diese Kollateralschäden werden in Kauf genommen, nur um mit Blick auf die erstrebte Sanktionierung einer Einzelperson wegen einer vermuteten Straftat den Sachverhalt aufzuklären oder den Aufenthaltsort des Beschuldigten zu ermitteln.

Die Ausnutzung von staatlicherseits geheim gehaltenen Sicherheitslücken ist durchaus keine düstere Fantasie, sondern bittere Realität.

Erst im Mai 2019 wurde bekannt, dass eine Sicherheitslücke in der Telefonfunktion bei WhatsApp genutzt wurde, um bei Zielpersonen eine Überwachungssoftware zu installieren und die Kontrolle über ihre Mobiltelefone zu gelangen. Vermutlich steckte hinter dem Angriff ein ausländischer Geheimdienst, Opfer war unter anderem ein Londoner Menschenrechtsanwalt,

> vgl. New York Times vom 13. 05.2019: WhatsApp Rushes to Fix Security Flaw Exposed in Hacking of Lawyer's Phone, Nicole Perlroth und Ronen Bergman, online abrufbar unter https://www.nytimes.com/2019/05/13/technology/nso-group-whatsapp-spying.html, zuletzt abgerufen am 01.07.2019.

Erinnert sei zudem an den Vorfall um „WannaCry" vom 12. Mai 2017: Innerhalb weniger Stunden infiltrierte dieses Schadprogramm, ein sog. Kryptotrojaner, weltweit etwa 220.000 Systeme. Der Trojaner verschlüsselte die Daten auf den betroffenen Computern und bot den Nutzern zeitgleich einen Code für die Entschlüsselung an, ansonsten werde die Löschung der

Daten veranlasst. In Deutschland war davon bspw. die Deutsche Bahn betroffen. Besonders schwer traf es das Gesundheitssystem in Großbritannien. Zahlreiche Rechner des National Health Service waren befallen. Patient*innen berichteten von chaotischen Zuständen. Die Daten von Krebs- und Herzpatient*innen standen nicht mehr zur Verfügung. Viele Kranke mussten in andere Kliniken umgeleitet werden.

Der WannaCry-Trojaner nutzte eine Lücke im Betriebssystem Microsoft Windows. Diese Lücke war schon Jahre zuvor von der National Security Agency, des auf Hacking spezialisierten US-Geheimdienstes, entdeckt, aber nicht an den Hersteller Microsoft gemeldet worden, damit er die Sicherheitslücke schließe. Brad Smith, Präsident von Microsoft, erhob in einer Erklärung den Vorwurf, die Geheimdienste würden diese Lücken absichtsvoll horten, statt sie sofort an die Hersteller zu melden.

Die Verfassungsbeschwerde rügt, dass die Beförderung dieser immensen Sicherheitsgefahren nicht mit dem Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG bzw. Art. 2 Abs. 1 GG) vereinbar ist. Der Einsatz von Staatstrojanern müsste vielmehr von einem Schwachstellen-Management begleitet werden, welches die Verwendung von bisher unbekannten Sicherheitslücken (sog. *0-days*) verbietet, solange der Hersteller des Systems nicht über die Lücke informiert ist und sicherzustellt, dass sich alle Behörden dafür einsetzen, ihnen bekannte Sicherheitslücken durch die Hersteller so schnellstmöglich schließen zu lassen.

Daraus resultiert auch keine erhebliche Beeinträchtigung der Gefahrenabwehr. Denn eine Sicherheitslücke, die dem Hersteller bereits bekannt ist, aber beispielsweise wegen Nachlässigkeit des Systembetreibers noch nicht geschlossen wurde, kann aus der Perspektive der IT-Sicherheit durch staatliche Stellen ausgenutzt werden. Gleiches gilt für Sicherheitslücken, die nicht auf Fehlern der Hersteller beruhen, sondern auf einer individuellen fehlerhaften Einrichtung des informationstechnischen Systems.

Darüber hinaus richtet sich die Verfassungsbeschwerde gegen die Ermächtigung zur automatisierten Datenanalyse in § 25a HSOG. Mit § 25a HSOG hat der Hessische Gesetzgeber eine gesetzliche Grundlage für die in Hessen genutzte Datenanalysesoftware „Gotham“ der Firma Palantir geschaffen, die von der Polizei Hessen unter der Bezeichnung hessenDATA (im Folgenden: Hessendata) genutzt wird. § 25a HSOG ermächtigt nicht zur Datenerhebung, sondern ermöglicht die gemeinsame Speicherung und den automatisierten Abgleich von Daten, die auf Grundlage anderer Ermächtigungsgrundlagen gewonnen wurden. Aus welchen Datenquellen die Daten stammen, die in die automatisierte Datenanalyse einfließen und insbesondere, welche externen Daten von anderen öffentlichen Stellen, privaten Unternehmen oder aus dem Internet einfließen, lässt sich weder dem Gesetzestext noch der Gesetzesbegründung entnehmen. Entsprechende Auskunftsersuche der Gesellschaft für Freiheitsrechte an das Hessische Landeskriminalamt und an das Hessische Innenministerium vom 08.04.2019 wurden mit Bescheid vom 11.04.2019 und 17.04.2019 abgelehnt. Auch auf mündliche Nachfrage der Gesellschaft für Freiheitsrechte beim Landesverband Hessen des Bunds deutscher Kriminalbeamter wurde bestätigt, dass zu diesen Fragen keine Auskunft gegeben werden könne.
Aus dem Untersuchungsausschuss des Hessischen Landtags zu Palantir ist bekannt, dass Hessendata Daten aus der polizeilichen Datenbank POLAS, dem polizeilichen Auskunftssystem, in dem die repressiven Daten gespeichert sind, der präventiven Datenbank CRIME, sowie aus dem Vorgangsbearbeitungssystem ComVor speichert. Darüber hinaus speichert Hessendata alle Verkehrsdaten aus der Telekommunikationsüberwachung sowie die von den Telekommunikationsanbietern zur Verfügung gestellte Daten. Auch Daten aus forensischen Extrakten,

beispielsweise beschlagnahmten Mobiltelefonen, werden in Hessendata gespeichert. Zudem fließen externe Quellen ein, konkret genannt wurden im Untersuchungsausschuss Informationen aus sozialen Netzwerken,

vgl. Zwischenbericht des Untersuchungsausschusses 19/3 zu Drucksache 19/6574 vom 03. Januar 2019, Seite 17.

Potenziell können in die automatisierte Datenanalyse alle Daten einfließen, die die Polizei Hessen selbst erheben kann oder die sie sich auf Grundlage von §§ 13 HSOG, 22 HDSIG von anderen öffentlichen Stellen oder privaten Unternehmen übermitteln lassen kann.
Welche Datenbestände für die Datenanalyse jeweils erforderlich sind, ist gemäß der Gesetzesbegründung anhand des jeweiligen Analysezwecks zu entscheiden,

LT-Drs. 19/6502, Seite 41.

Die gespeicherten Daten aus den vorgenannten Quellen können mithilfe von Hessendata gemeinsam analysiert werden. Gemäß § 25a Abs. 2 HSOG dient die automatisierte Datenanalyse dazu, „Beziehungen oder Zusammenhänge zwischen Personen, Personengruppierungen, Institutionen, Organisationen, Objekten und Sachen“ herzustellen und die „eingehenden Erkenntnisse zu bekannten Sachverhalten [zuzuordnen] und gespeicherte Daten statistisch auszuwerten“.

Hessendata besteht aus der „Revisioning Database“, wo die Daten aus den verschiedenen Quellen gespeichert werden und der In-Memory-Datenbank namens „Horizon“, auf der die Analytiker ihre Auswertungen durchführen, hinzu kommen die Nutzeranwendungen und die im Hintergrund arbeitenden Systemdienste,

vgl. Produktbeschreibung Gotham, online abrufbar unter https://www.palantir.com/palantir-gotham/principles/, https://www.palantir.com/palantir-gotham/platform-features/, zuletzt abgerufen am 01.07.2019.

Es ist zu vermuten, dass zusätzlich zum Abbild vorhandener Datenquellen in Hessendata weitere Informationen gespeichert werden, die sich aus der Analyse ergeben. Dies können beispielsweise neue Erkenntnisse sein, die in den bisher verstreut gespeicherten Daten nicht erkennbar waren oder durch die Verknüpfung mit externen Daten, beispielsweise aus sozialen Medien zutage treten. Treffer in externen Quellen werden dann in die „Revisioning Database“ übernommen und dort gespeichert,

vgl. Produktbeschreibung Gotham: „Palantir Gotham offers a single point of search across internal and external data sources. During discovery, users can explore data in its original format, as well as in an enriched view only available in Palantir Gotham. The platform's federation capability seamlessly integrates external systems so they continue to add value to the data ecosystem. Users can promote external records to fuse them with the intelligence in Gotham, and relevant data is automatically surfaced to users for review, which simplifies analysis of large-scale data.“, online abrufbar unter https://www.palantir.com/palantir-gotham/principles/, zuletzt abgerufen am 02.07.2019.

Über die Anwendungen können die Nutzer mit der Analyseplattform kommunizieren, dort Eingaben machen oder Auswertungen durchführen. Dazu gehört beispielsweise „Graph“ zur Darstellung von Beziehungsnetzen, „Geo“ für die Darstellung und Anzeige auf Karten, sowie ein „Object Explorer“ und ein „Browser“,

> vgl. Produktbeschreibung Gotham, online abrufbar unter www.palantir.com/palantir-gotham/platform-features/, zuletzt abgerufen am 01.07.2019.

Zwischen den Datenspeichern und den Anwendungen, mit denen die Nutzer arbeiten, wirken im Hintergrund Systemdienste. Beispielsweise führen die Dienste Raptor und Phoenix im Hintergrund eine Verbundsuche auf externen Datenquellen aus. Intransparent ist derzeit, welche externen Datenquellen in Hessendata für diese Dienste zur Verfügung stehen und ob der Datenabruf bei externen Quellen automatisiert erfolgt,

> “To help organizations maintain control and ownership over their data assets, our engineers have developed two main federated data solutions, Raptor and Phoenix, that allow users to search data that is not stored within Palantir Gotham”, Palantir Gotham, Upholding Data Protection Regulations in the European Union, online abrufbar unter https://wget2014.files.wordpress.com/2014/04/16_palantir-gotham-upholding-data-protection-regulations-in-the-european-union.pdf, zuletzt abgerufen am 01.07.2019.

§ 25a Abs. 1 HSOG normiert die Eingriffsschwelle für die Nutzung der automatisierten Datenanalyse. Demnach ist die Anwendung beschränkt auf begründete Einzelfälle zur „vorbeugenden Bekämpfung von in § 100a Abs. 2 StPO genannten Straftaten oder zur Abwehr einer Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder Leib, Leben oder Freiheit einer Person oder Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist, oder wenn gleichgewichtige Schäden für die Umwelt zu erwarten sind“.

Gerade die vorbeugende Straftatenbekämpfung verlagert die Anwendung ins Vorfeld einer konkreten Gefahr. Dies entspricht auch dem Zweck der Analyse, die dazu dient, Zusammenhänge und Handlungsmuster zu erschließen und so auch zukünftige Gefahren zu erkennen. Dieser Anwendungsbereich im Vorfeld einer konkreten Gefahr wird auch in der Gesetzesbegründung bestätigt. Danach ermöglicht diese Form der Datenanalyse die Gewinnung wesentlicher Anhaltspunkte für Gefahren und bevorstehende Straftaten,

> LT- Drs. 19/6502, Seite 41.

Nicht näher benannt ist in § 25a HSOG der Kreis der Betroffenen, aus der Natur der Datenanalyse ergibt sich jedoch zwangsläufig, dass diese nicht auf den unmittelbaren Störer beschränkt bleibt. Schließlich soll die Analyse Erkenntnisse über „gemeinsame Strukturen, Handlungsmuster, Personengruppen und zeitliche, sachliche, organisatorische, personale und situative Zusammenhänge“ bringen,

> LT- Drs. 19/6502, Seite 41.

Da die Software Verknüpfungen, Netzwerke und Strukturen erst zutage fördern soll, ist von den Analysen unweigerlich ein weiter Personenkreis betroffen. Schließlich kann jede Beziehung eines Objekts mit einem anderen Objekt zur Auswertung herangezogen werden und dies führt zu weiteren Objekten, die wieder mit anderen Objekten in Beziehung stehen,

> anschaulich macht dies ein Artikel der Frankfurter Rundschau, der am 02.07.2018 nach der Vorstellung von hessenDATA durch die Frankfurter Polizei erschien. „Projektleiter Bodo Koch" [demonstrierte] „wie die Software den Ermittlern Netzwerke von Personen anzeigt, die etwa vom Handy eines Verdächtigen angerufen wurden oder in der Nähe einer beobachteten Wohnung leben. Auch Polizeifotos der Menschen aus dem Umfeld sind abrufbar". Pitt v. Bebenburg: Beuth verteidigt Analysesoftware der Polizei, online abrufbar unter https://www.fr.de/rhein-main/spd-org26325/beuth-verteidigt-analysesoftware-polizei-11034270.html, zuletzt abgerufen am 01.07.2019 , vgl. auch den Bericht der Süddeutschen Zeitung vom 18. Oktober 2018: Jannis Brühl, „Palantir in Deutschland. Wo die Polizei alles sieht", online abrufbar unter https://www.sueddeutsche.de/digital/palantir-in-deutschland-wo-die-polizei-alles-sieht-1.4173809, zuletzt abgerufen am 01.07.2019.

Als flankierende Verfahrenssicherungen sieht § 25a Abs. 3 HSOG lediglich vor, dass die Einrichtung und wesentliche Änderung einer automatisierten Anwendung zur Datenanalyse durch Anordnung der Behördenleitung oder einer*s von dieser beauftragten Bediensteten erfolgen muss und vor Einrichtung oder Änderung der Hessische Datenschutzbeauftragte anzuhören ist. Vorgaben zur Dauer der Anwendung, Erneuerung der Anwendung, Löschung der Daten, sowie zum Grundsatz der Zweckbindung trifft § 25a HSOG selbst keine Aussagen. Die Gesetzesbegründung führt dazu aus, dass in Bezug auf die Speicherung und Nutzung der Daten in Hessendata die allgemeinen Regelungen des § 20 HSOG zur Datenweiterverarbeitung, Zweckbindung, zum Grundsatz der hypothetischen Datenneuerhebung zu beachten sind,

> Hessischer Landtag, Drs. 19/6502, Seite 41.

Die Verfassungsbeschwerde rügt die Eingriffsschwelle des § 25a HSOG, die angesichts der Intensität des Grundrechtseingriffs zu weit ist. § 25a HSOG weist eine große Streubreite auf und ermöglicht die Erzeugung nahezu umfassender Persönlichkeitsprofile. Gemessen daran ist die Eingriffsermächtigung unverhältnismäßig, insbesondere ist sie hinsichtlich der Gefahrenschwelle und der geschützten Rechtsgüter zu weit. Zudem fehlt es an den erforderlichen Verfahrenssicherungen.

III. Die Beschwerdeführer*innen

1. Beschwerdeführerin zu 1

Die Beschwerdeführerin zu 1 lebt in Kassel und ist Lehrerin in Ruhestand. Sie stammt aus einer jüdischen Familie, ihr Vater Peter Gingold war nach seiner Flucht aus Deutschland im französischen Widerstand gegen den Nationalismus aktiv. 1947 gründete er gemeinsam mit

anderen Verfolgten die „Vereinigung der Verfolgten des Naziregimes“ (VVN-BdA). Die Beschwerdeführerin zu 1 ist bis heute in der VVN-BdA aktiv und gewähltes Mitglied des Sprecher*innenrats der Landesvereinigung Hessen der VVN-BdA. Die VVN-BdA versteht sich als überparteiliche Sammelorganisation von Menschen, die gegen neofaschistische, rassistische und nationalistische Bestrebungen eintreten. Obwohl die VVN-BdA im Jahresbericht des Landesamts nicht namentlich genannt wird, steht die VVN-BdA nach Angaben des Landesamts gleichwohl in Hessen ebenso wie in zahlreichen anderen Bundesländern unter Beobachtung. Das Landesamt begründet dies mit dem Streben der VVN-BdA nach einer sozialistischen Gesellschaft, was eine Beeinträchtigung der freiheitlich demokratischen Grundordnung darstelle,

> vgl. VG Kassel, Urteil vom 15.10.2017, Az. 4K641/13.KS, Seite 8 und 13, Klageerwiderung des Landesamts vom 07. Oktober 2016, VG Kassel Az. 4K64fl/13.KS, Seite 18.

Die Beschwerdeführerin zu 1 ist dem Landesamt nachweislich auch persönlich bekannt und wird bis heute vom Landesamt beobachtet,

> vgl. VG Kassel, Urteil vom 15.10.2017, Az. 4K641/13.KS.

Schon seit ihrer Jugend engagiert sich die Beschwerdeführerin zu 1 gemeinsam mit ihrer Familie gegen Krieg und Faschismus. 1975 wurde die Beschwerdeführerin aus dem Schuldienst entlassen und bekam ein Berufsverbot. Maßgeblich für das Berufsverbot, waren Erkenntnisse des Verfassungsschutzes zu Teilnahmen an Demonstrationen gegen den Krieg in Vietnam, Verteilungen von Flugblättern gegen Krieg und Faschismus und Reisen in die DDR.

Bis heute ist die Beschwerdeführerin zu 1 zu friedenspolitischen und antifaschistischen Themen politisch aktiv. Sie ist Sprecherin des Landesausschusses der VVN-BdA Hessen und tritt regelmäßig auf Veranstaltungen der VVN-BdA auf, beispielsweise führt sie gemeinsam mit der VVN-BdA Lesereisen zur Autobiographie ihres Vaters durch,

> vgl. den ausführlichen Bericht über die Beschwerdeführerin zu 1 vom 02.04.2019 auf Deutschlandfunkkultur, online abrufbar unter https://www.deutschlandfunkkultur.de/silvia-gingold-und-ihr-kampf-gegen-den-verfassungsschutz.3720.de.html?dram:article_id=441565, zuletzt abgerufen am 01.07.2019.

Zudem ist sie aktives Mitglied im Kasseler Friedensforum und nimmt regelmäßig an antifaschistischen und friedenspolitischen Demonstrationen, Aktionen und Veranstaltungen teil. Im Rahmen ihres politischen Engagements steht sie regelmäßig im Austausch mit Mitgliedern von Organisationen, die vom Landesamt als linksextremistisch eingestuft werden, wie beispielsweise die DKP.

Seit 2009 wird beim Landesamt eine Personenakte zur Beschwerdeführerin zu 1 geführt. Dies brachte sie durch eine Anfrage vom 16.10.2012 an das Landesamt in Erfahrung. Mit Antwort vom 18.11.2012 teilte man ihr mit, dass sie seit 2009 im Bereich Linksextremismus gespeichert sei und wies auf eine Lesung aus der Autobiographie ihres Vaters im Rahmen der Gegenbuchmesse am 15.10.2011 und einen Redebeitrag zu den Berufsverboten auf der Demonstration „staatliche Unterstützung für Nazis beenden-Verfassungsschutz auflösen“ am 28.01.2012 hin.

Mehr Angaben machte das Landesamt nicht und verwies darauf, dass das Auskunftsinteresse der Klägerin hinter das öffentliche Interesse an der Geheimhaltung der Tätigkeiten des Landesamts zurücktrete,

> vgl. Schreiben des Landesamts für Verfassungsschutz Hessen vom 08.11.2012, Az. DSB-038-S-470 000-338/2012.

Die Beschwerdeführerin erhob 27.05.2013 Klage gegen das Landesamt und verlangte vollumfängliche Auskunft über die über sie erhobenen Daten sowie Löschung dieser Daten. Die Klage wurde mit Urteil vom 15.10.2017 abgewiesen, die Klägerin hat beim VGH Kassel einen Antrag auf Zulassung der Berufung gestellt,

> vgl. VG Kassel, Urteil vom 15.10.2017, Az. 4K641/13.KS.

Auch im Rahmen des Gerichtsverfahrens hat das Landesamt die personenbezogenen Daten der Beschwerdeführerin nicht offengelegt, über 100 Seiten der Akte waren überwiegend geschwärzt. Das Landesamt hat im Rahmen des Verwaltungsgerichtsverfahrens am 07.10.2013 eine Sperrerklärung für nicht vorgelegte Bestandteile der Akte abgegeben. Die Vorenthaltung weiter Teile der Personenakte ist im Rahmen eines In-Camera-Verfahrens überwiegend vom Hessischen VGH bestätigt worden,

> vgl. Hess. VGH, Beschluss vom 16.03.2016, Az. 27F1817/15.

In der Sperrerklärung begründet das Landesamt die Geheimhaltung zum Teil teilweise mit Quellen- und Informantenschutz. Viele der Informationen stammten demnach aus persönlichen Gesprächen, Emails oder von Veranstaltungen, deren Teilnehmerkreis klein gewesen sei,

> Sperrerklärung des Landesamts für Verfassungsschutz Hessen nach § 99 Abs. 1 Satz 2 VwGO vom 07.10.2013.

Diese Sperrerklärung weist darauf hin, dass im direkten Umfeld der Beschwerdeführerin auch verdeckte Ermittler*innen und Vertrauenspersonen eingesetzt werden.

Die Beschwerdeführerin zu 1 nutzt im Rahmen ihres politischen Engagements komplexe informationstechnische Systeme wie PCs und Laptops, verfügt über einen Internetzugang und hat ein internetfähiges Mobiltelefon. Sie verreist gelegentlich mit dem Flugzeug, häufiger mit der Bahn oder dem Reisebus.

2. Beschwerdeführer zu 2

Der Beschwerdeführer zu 2 lebt in Mörfelden-Walldorf und ist Sprecher der Vereinigung der Verfolgten des Naziregimes – Bund der Antifaschistinnen und Antifaschisten (VVN-BdA) in Hessen. Als Lehramtsanwärter erhielt der Beschwerdeführer zu 2 1974 ein Berufsverbot und hat in Folge dessen auch in späteren Jahren keine Stelle als Lehrer gefunden. Dem Berufsverbot lag die Mitgliedschaft in der DKP, die Teilnahme an Demonstrationen zum Umweltschutz und sein Engagement in der Deutschen Friedensgesellschaft – Vereinigte KriegsdienstgegnerInnen (DFG-VK) zugrunde. Zwischen 1976 und 1979 arbeitete der Beschwerdeführer zu 2 im Präsidium der VVN-BdA im Organisationsbereich. Zwischen 1979 und 2013 war er als Pädagoge bei der IG Metall beschäftigt. Seitdem ist er in Rente.

Der Beschwerdeführer zu 2 ist als Sprecher aktives Mitglied der VVN-BdA Hessen und betreut als Webmeister den Internetauftritt der Organisation. Im Rahmen der VVN-BdA Hessen organisiert und beteiligt er sich an gemeinsamen Kundgebungen und Demonstrationen. Zuletzt nahm er beispielsweise an der Protestkundgebung gegen die Afd am 24.05.2019 in Frankfurt und an der Demonstration „Ein Europa für alle! Deine Stimme gegen Nationalismus“ am 19.05.2019 in Frankfurt teil.

Mittlerweile ist der Beschwerdeführer zu 2 nicht mehr DKP-Mitglied, aber eng mit der Partei und ihren Mitgliedern verbunden, die im Stadtparlament von Mörfelden-Walldorf als Zusammenschluss DKP-Linke Liste 13,8% der Stimmen erhielt und 6 Sitze hat. Unter anderem hat er für den Wahlkampf 2016 die Internetseite der örtlichen DKP-Linke Liste gestaltet. Im Komitee „40 Jahre Berufsverbote“ setzt er sich gegen die Nachwirkungen der Berufsverbote ein und hat sich in diesem Zusammenhang beim hessischen Landesamt für Verfassungsschutz erkundigt, welche Daten über ihn vorliegen. Am 7. Juni 2018 erhielt der Beschwerdeführer zu 2 auf Nachfrage beim Landesamt für Verfassungsschutz die Auskunft, dass über ihn Daten im Phänomenbereich Linksextremismus gespeichert sind. Diese Daten umfassten seine Stellung als Mitglied im Sprecher*innenrat der VVN-Bda und seine Funktion als Webmaster der Internetseiten der VVN-BdA Hessen und der Internetseite der DKP-Linke Liste Mörfelden-Walldorf,

> Erkenntnismitteilung des Landesamts vom 07.06.2019, Az: DSB-038-S-470 000-725/2018.

In der Akte des Landesamts für Verfassungsschutz der Beschwerdeführerin zu 1 taucht der Beschwerdeführer zu 2 ebenfalls auf, als Teilnehmer an einer Demonstration gegen die NSU und zu 40 Jahren Berufsverbote im Jahr 2012.

Der Beschwerdeführer zu 2 nutzt im Rahmen seines politischen Engagements informationstechnische Systeme wie PCs und Laptops, verfügt über einen Internetzugang und hat ein internetfähiges Mobiltelefon. Er verreist gelegentlich mit dem Flugzeug, der Bahn oder dem Reisebus und nutzt auch Carsharingdienste.

3. Beschwerdeführerin zu 3

Die Beschwerdeführerin zu 3 ist Strafverteidigerin in Frankfurt. Sie vertritt etliche Personen, denen vorgeworfen wird, ausländischen terroristischen Vereinigungen anzugehören oder sie zu unterstützen, darunter unter anderem auch Sami A., dessen Fall bundesweit Aufsehen erregte, weil er im Juli 2018 trotz einer entgegenstehenden Entscheidung des Verwaltungsgerichts Gelsenkirchen abgeschoben wurde. Ein weiteres exemplarisches Verfahren ist die Verteidigung eines der Angeklagten im Prozess vor dem Oberlandesgericht München gegen angebliche Mitglieder bzw. Unterstützer der Organisation Ahrar al-Sham. Einen anderen Mandanten, dem ebenfalls die Unterstützung dieser nach den §§ 129a, 129b StGB verfolgten Organisation vorgeworfen wird, hat sie vor dem Bundesverfassungsgericht vertreten, um seine Abschiebung nach Tunesien zu verhindern. Zudem ist sie die Strafverteidigerin von Jennifer W., die sich vor vier Jahren im Irak dem IS angeschlossen haben soll und wegen Mordes und Begehung von Kriegsverbrechen vor dem OLG München angeklagt ist.

Weiterhin vertritt die Beschwerdeführerin zu 3 Yasmin H., die im Februar 2019 vor dem OLG Düsseldorf wegen des vorsätzlichen Herstellens einer biologischen Waffe und der Vorbereitung einer schweren staatsgefährdenden Gewalttat angeklagt wurde. Ein weiterer Mandant ist Malik F., ehemaliger Doktorand an der Universität Darmstadt, gegen den gerade ein Verfahren vor dem OLG Frankfurt läuft, wo er sich wegen des Werbens für den IS und dreier weiterer Taten verantworten muss. Das Verfahren gegen Bilal G., einem der wesentlichen Organisatoren hinter der Koranverteilaktion „Lies!“, im Frühjahr 2018 vor der Staatsschutzkammer des Landgerichts Frankfurt am Main ist noch nicht rechtskräftig abgeschlossen. Dem Achtundzwanzigjährigen wurde Beihilfe zur Vorbereitung einer schweren staatsgefährdenden Gewalttat vorgeworfen. Schließlich vertritt die Beschwerdeführerin zu 3 Sarah O., gegen die im April 2019 vor der Staatsschutzkammer des OLG Düsseldorf Anklage erhoben wurde, unter anderem wegen Mitgliedschaft in einer terroristischen Vereinigung, Menschenhandel und Freiheitsberaubung. Sie soll im Jahr 2013 nach Syrien ausgereist und sich dort dem IS angeschlossen haben. Von dort aus soll sie versucht haben auch weitere Personen zur Ausreise aus Europa und nach Syrien zu bewegen.
Die Beschwerdeführerin zu 3 hat zudem im Prozess gegen den rechtsterroristischen Nationalsozialistischen Untergrund die Familie eines der Mordopfer vertreten.

Da die meisten Staatsschutzverfahren, in denen die Beschwerdeführerin zu 3 mandatiert ist, einen erheblichen Auslandsbezug aufweisen, ermittelt sie auch im Ausland, um Zeugen zu finden und zu befragen. Sie unterhält in der Folge Kontakte zu zahlreichen mutmaßlichen Angehörigen terroristischer Vereinigungen im In- und Ausland.

Die Beschwerdeführerin zu 3 erledigt ihre Anwaltsgeschäfte per Telefon und Computer, sie nutzt zudem Chatdienste wie Whatsapp.

Anlässlich der Vertretung des als Gefährder eingestuften Sami A. hat die Beschwerdeführerin seit August 2018 vier Drohschreiben erhalten. Teils enthielten diese Schreiben Daten, die nicht öffentlich bekannt sind, wie den vollen Namen und das Geburtsdatum der zweijährigen Tochter und die genaue Wohnadresse der Familie oder Namen und Geburtsdaten der Eltern und des Ehemanns. Die Behörden ermittelten daraufhin, dass Daten der Anwältin kurz vor Versendung des ersten Drohschreibens an einem Computer im 1. Polizeirevier Frankfurt abgefragt worden waren,

> vgl. Zeit-Online vom 05.02.2019, online abrufbar unter https://www.zeit.de/politik/deutschland/2019-02/seda-basay-yildiz-drohbrief-frankfurter-rechtsanwaeltin-rechtsextremismus, zuletzt abgerufen am 01.07.2019.

4. Beschwerdeführer zu 4

Der Beschwerdeführer zu 4 ist Rechtsanwalt in Gießen, insbesondere ist er im Polizei- und Versammlungsrecht sowie als Strafverteidiger tätig. Er vertritt regelmäßig Menschen aus dem linken Spektrum. Er vertrat beispielsweise Betroffene in mehreren Strafverfahren und verwaltungsgerichtlichen Verfahren im Zusammenhang mit den „Blockupy“-Demonstrationen in Frankfurt und den Ereignissen anlässlich des G20-Gipfels in Hamburg. Im Versammlungsrecht unterstützt er Organisationen und Initiativen bei der Anmeldung von Versammlungen

und geht gegen polizeiliche Auflagen und andere Einschränkungen des Versammlungsrechts vor.

Nicht wenige seiner Mandant*innen werden vom Verfassungsschutz beobachtet und sind aufgrund verschiedener Strafverfahren und Überwachungsmaßnahmen in diversen Polizeidatenbanken gespeichert. Verfahren, in denen die verlässliche Löschung der von der Polizei gespeicherten Daten beansprucht worden sind, waren vor den Verwaltungsgerichten erfolglos.

In mehreren Ermittlungsverfahren gegen Mandant*innen des Beschwerdeführers zu 4 ist sein dienstliches Mobiltelefon abgehört, Gespräche mit Mandant*innen mitgehört und protokolliert worden. Dies brachte die Akteneinsicht zutage. In keinem der Fälle konnte in den Strafprozessen erreicht werden, dass die auf diese Art und Weise
erlangten Ermittlungsergebnisse einem Beweisverwertungsverbot unterlagen. So beispielsweise in einem Strafverfahren eines Pastoralreferenten aus Hessen, den der Beschwerdeführer zu 4. vertrat. Dieser Mandant wurde beschuldigt, für einen von Neonazis verübten Brandanschlag verantwortlich gewesen zu sein. Aus den Ermittlungsakten ergab sich, dass die vom Beschwerdeführer zu 4. mit dem Pastoralreferenten geführten Telefongespräche überwacht worden sind.

Der Beschwerdeführer zu 4 engagiert sich auch außerhalb seiner anwaltlichen Tätigkeit bürgerrechtlich. Er ist zweiter Vorsitzender des Landesverbandes der Humanistischen Union Hessen und nimmt regelmäßig an antifaschistischen Demonstrationen teil.

Im Rahmen seines politischen Engagements pflegt der Beschwerdeführer Kontakte zu Organisationen und Menschen, die vom Verfassungsschutz beobachtet werden, unter anderem kurdische Exilanten und antifaschistische Gruppen in ganz Mittelhessen. Hervorzuheben ist seine Tätigkeit im Ermittlungsausschuss Frankfurt am Main, dessen Aufgabe es unter anderem ist, polizeiliche Übergriffe auf Versammlungsteilnehmer zu dokumentieren.

Am 29.05.2019 beantragte der Beschwerdeführer zu 4 bei der Generalstaatsanwaltschaft Frankfurt am Main, dass ihm die Daten über die Funkzellenabfragen zu seiner Mobilfunknummer mitgeteilt werden. Den Antrag stützte er auf § 101 IV StPO. Der Antrag ging am 22.05.2017 bei der Generalstaatsanwaltschaft in Frankfurt am Main ein. Die begehrten Auskünfte sind bis heute nicht erteilt worden.

Der Beschwerdeführer zu 4 verwendet für seine Arbeit mehrere Computer sowie ein internetfähiges Mobiltelefon. Mit Mandant*innen kommuniziert der Beschwerdeführer zu 4 überwiegend per Mail, seine Mailadresse ist an verschiedenen Stellen im Internet öffentlich vermerkt, so dass sie auch einem Erstkontakt offensteht. Zudem nutzt er verschiedene Messengerdienste.

5. Beschwerdeführer zu 5

Der Beschwerdeführer zu 5 ist Journalist und lebt in Marburg. Der Beschwerdeführer hat zwölf Jahre lang als freier Mitarbeiter für den Hessischen Rundfunk, für das Deutschlandradio und die ARD sowie zahlreiche andere Medien gearbeitet und ist derzeit Redaktionsleiter der Onlinezeitung Marburg.news.

Der Beschwerdeführer zu 5 recherchiert und schreibt Berichte zu aktuellen Themen aus Gesellschaft und Politik, Überwachung und Bürgerrechte. Er berichtet häufig über politisch „links“ ausgerichtete Gruppierungen.

Dazu kommuniziert er nicht selten mit Menschen, die mit einiger Wahrscheinlichkeit vom Landesamt oder der hessischen Polizei beobachtet werden. Dies ist in einem Fall bereits aktenkundig geworden. Dort sind Telefonate des Beschwerdeführers zu 5 mit einem Journalisten überwacht worden, weil letzterer aufgrund eines Ermittlungsverfahrens über einen Zeitraum von mindestens drei Monaten einer Überwachung seiner Telekommunikation ausgesetzt war,

> vgl. Presseerklärung der Humanistischen Union Marburg vom 28.02.2013, http://hu-marburg.de/2013/02/28/pm-313-journalisten-und-buergerrechtler-ueberwacht-hu-marburg-empoert-ueber-abhoermassnahme/#main, zuletzt abgerufen am 01.07.2019.

In seiner journalistischen Arbeit pflegt der Beschwerdeführer zu 5 auch regelmäßige Kontakte zu regimekritischen Personen aus Syrien und der Türkei, Russland, China, Ägypten, Eritrea und Äthiopien.

Der Beschwerdeführer zu 5 hält sich einen Großteil des Jahres in Marburg auf und hat dort etliche politisch aktive Freunde und Bekannte. Er ist dort auch selbst politisch aktiv, als stellvertretender Landessprecher der Humanistischen Union Hessen und Vorsitzender der Humanistischen Union Marburg, sowie als Vorsitzender des Arbeitskreis Barrierefreies Internet (AKBI). Im Rahmen seines politischen Engagements steht der Beschwerde im Kontakt zu zahlreichen Personen, die unter Beobachtung des Landesamts stehen und zu denen umfangreiche personenbezogene Daten in Polizeidatenbanken gespeichert sind,

> beispielsweise fand am 27.05.2014 fand eine Veranstaltung der Humanistischen Union Marburg mit der Kletteraktivistin Cecile Lecomte statt, die 2015 vom Landeskriminalamt Niedersachsen erfuhr, dass sie als sog. „relevante Person“ eingestuft war. Informationen zur Veranstaltung online abrufbar unter http://hu-marburg.de/2014/05/28/kommen-sie-da-runter-eichhoernchen-cecile-lecomte-stellte-buch-ueber-kletteraktionen-vor/ , zuletzt abgerufen am 01.07.2019.

Die Humanistische Union Marburg und in seiner Funktion als Vorsitzender auch der Beschwerdeführer zu 5 selbst unterhalten auch verschiedene Kontakte zu ausländischen Dissidenten und Regimekritikern, beispielsweise aus Syrien und der Türkei,

> so veranstaltete die Humanistische Union Marburg am 17.12.2016 gemeinsam mit Oppositionellen aus Syrien eine Mahnwache gegen das Trauma von Krieg, Vertreibung und Flucht, Informationen dazu online abrufbar unter http://hu-marburg.de/2016/12/18/gut-60-menschen-bei-mahnwache-fuer-gefluechtete-erfolgreiche-aktion-gegen-das-trauma-von-krieg-vertreibung-und-flucht/, sowie am 22.02.2013 eine Veranstaltung zur Pressefreiheit in der Türkei, Informationen dazu online abrufbar unter http://hu-marburg.de/2013/02/18/pm-213-politisch-gewollt-strafrechtliche-verfolgung-von-rechtsanwaelten-in-der-tuerkei/, zuletzt abgerufen am 01.07.2019.

Zudem unterhält der Beschwerdeführer zu 5 seit vielen Jahren enge persönliche Kontakte zu regierungskritischen Aktivist*innen aus den USA, die sich dort in Friedensgruppen und im

Umweltschutz betätigen. Als Ansprechpartner des HU-Arbeitskreises "Psychiatrie" wird der Beschwerdeführer immer wieder in sehr persönlichen Angelegenheiten angesprochen, die absolutes Vertrauen erfordern.

Der Beschwerdeführer zu 5 ist blind und dadurch darauf angewiesen, sich alle seine Notizen am Computer zu machen. Es ist ihm nicht möglich, besonders vertrauliche Informationen in Notizbüchern oder auf Zetteln aufzuschreiben und an unterschiedlichsten Stellen aufzubewahren. Da der Beschwerdeführer zu 5 nur in Begleitung mobil ist, führt er seine Kommunikation fast ausschließlich telefonisch oder per Mail. Zudem nutzt er verschiedene Messenger- und Social-Media-Dienste.

6. Beschwerdeführer zu 6

Der Beschwerdeführer zu 6 vereint in seiner Person verschiedene Positionen, die mit dem Zugriff auf große Mengen hochsensibler Daten einhergehen. Er ist Mitglied im Aufsichtsrat der DE-CIX Management GmbH, die in Frankfurt den größten deutschen Internetknoten betreibt. An diesem Internetknoten passieren die Datenströme der größten Internet-Provider weltweit. Als Aufsichtsratsmitglied der DE-CIX ist er Empfänger einer Vielzahl sensibler Daten, die auf seinem persönlichen Computer zusammenlaufen. Dazu gehören unter anderem die Anordnungen des Bundesinnenministeriums (BMI), mit denen DE-CIX verpflichtet wird, Milliarden Datensätze von Internet-Nutzern an den BND auszuleiten sowie die E-Mails des BND, in denen die Abhörziele weiter konkretisiert werden. Damit verfügt der Beschwerdeführer zu 6 über als Verschlusssache eingestufte Informationen über drohende Gefahren für die freiheitliche demokratische Grundordnung oder den Bestand oder die Sicherheit des Bundes oder eines Landes, die sich aus den Anordnungen vom BMI und BND ergeben.

Zudem ist der Beschwerdeführer zu 6 bei mehreren Internetdienstanbietern Sicherheitsbeauftragter im Sinne des § 109 TKG und dort für die Sicherheit der Dienste und Systeme verantwortlich. Dadurch hat Beschwerdeführer zu 6 über seinen Computer Zugriff auf die Managementsysteme dieser Kunden und damit auf zahllose Kundenkonten und Kundendaten. Sein Aufgabenfeld als Sicherheitsbeauftragter umfasst auch die Telefondienste, auf die der Beschwerdeführer zu 6 zur Ausübung seiner Pflichten weitreichende Zugangsrechte hat. So ist es beispielsweise seine Aufgabe, die Schnittstellen für die staatliche Telekommunikationsüberwachung einzurichten.

Unter anderem ist der Beschwerdeführer zu 6 Sicherheitsbeauftragter und Datenschutzbeauftragter der Nexiu GmbH, einem Internetdienstanbieter aus Wehrheim in Hessen, der ca. 2500 Haushalte mit Internet und Telefondiensten versorgt. Er kann im Rahmen seines Auftrags auf die Daten und Adressen aller Kunden zugreifen, zudem über den Zugriff auf die Router und die Telekommunikation auch theoretisch alle Verkehrsdaten der jeweiligen Kunden einsehen.

Der Beschwerdeführer zu 6 ist zudem Sicherheitsbeauftragte und Datenschutzbeauftragter der Northern Access GmbH aus dem niedersächsischen Liebenau. Die gesamte Landkreisverwaltung des Landkreises Nienburg einschließlich Polizei, Einwohnermeldeamt, Kfz-Zulassungsstelle und ähnlichem werden von der Northern Access GmbH mit Breitbandanschlüssen versorgt. Als Sicherheitsbeauftragter der Northern Access GmbH hat der Beschwerdeführer zu 6 prinzipiell Zugriff auf weite Teile des internen Datenverkehrs des Landkreises Nienburg.

Der Beschwerdeführer zu 6 ist darüber hinaus stellvertretender Vorstandsvorsitzender und der verantwortliche Vorstand für Infrastruktur und Netze bei ECO, dem Verband der Internetwirtschaft. Dort kommunizieren die Mitglieder untereinander über aktuelle Entwicklungen in der Internetwirtschaft, beispielsweise tauschen sich die Mitglieder auch zu Sicherheitsfragen und aktuellen Sicherheitslücken aus. Der Verband ECO bringt sich regelmäßig mit fachlicher Expertise in aktuelle politische Entscheidungsprozesse und Debatten ein. Zu diesem Zweck erhalten die Vorstandsmitglieder regelmäßig vertrauliche Unterlagen aus der Politik, ebenso wie von Journalisten, die eine externe Beurteilung wünschen. Für seine qualifizierten Stellungnahmen greift der Vorstand auf die Erfahrungen der Verbandsmitglieder zurück und erhält zu diesem Zweck von den Mitgliedern vertrauliche Unterlagen, die regelmäßig auch Geschäftsgeheimnisse enthalten.

In sämtlichen beschriebenen Funktionen ist der Beschwerdeführer zu 6 persönlich benannt. Er ist als persönliches Mitglied in den Aufsichtsrat der DE-CIX GmbH und in den Vorstand des ECO-Verbandes gewählt worden, wie gesetzlich vorgesehen ist er auch persönlich als Sicherheitsbeauftragter verschiedener Unternehmen benannt worden.

Weil er aus beruflichen Gründen häufig auf Reisen ist, laufen sämtliche Kommunikationen auf dem Notebook des Beschwerdeführers zusammen.

Der Beschwerdeführer zu 6 nutzt in seiner Mailkommunikation Ende-zu-Ende Verschlüsselung und trifft auch darüber hinaus alle nach dem Stand der Technik möglichen Sicherheitsvorkehrungen, um seinen Datenbestand und seine Kommunikation zu sichern.

7. Beschwerdeführerin zu 7

Die Beschwerdeführerin zu 7 ist eine als GmbH organisierte Gesellschaft, die ihren Kund*innen IT-Sicherheitsdienstleistungen und den Betrieb von IT-Sicherheitsinfrastruktur anbietet, wie beispielsweise „Managed Firewalls“, „Gateways“ oder Proxies. Es gehört zum Kerngeschäft der Beschwerdeführerin zu 7, die IT-Infrastruktur ihrer Kund*innen frei von Fehlern wie Sicherheitslücken zu halten und diese auftretende Sicherheitslücken so schnell wie möglich zu schließen. Als Sicherheitsdienstleisterin hat die Beschwerdeführerin zu 7 Zugriff auf die IT-Systeme einiger ihrer Kund*innen, ein erfolgreicher Hackerangriff auf ihre Systeme könnte durch eine Hintertür auch den Datenverkehr einer Vielzahl von Kund*innen abgreifen.

C. Zulässigkeit

Die Verfassungsbeschwerde ist zulässig.

I. Frist

Die Jahresfrist des § 93 Abs. 3 BVerfGG ist gewahrt. Die Verfassungsbeschwerde richtet sich gegen Neuregelungen im HVSG und HSOG, die durch Artikel 1 und Artikel 3 des Gesetzes

zur Neuausrichtung des Verfassungsschutzes in Hessen (am 03. Juli 2018 veröffentlicht im Gesetz- und Verordnungsblatt für das Land Hessen, S. 302.) eingeführt wurden. Bei einer Gesetzesänderung wird die Jahresfrist des § 93 Abs. 3 BVerfGG neu in Lauf gesetzt, wenn der Gesetzgeber das materielle Gewicht einer Regelung verändert, den Anwendungsbereich einer Norm eindeutiger als bisher bestimmt, ihn grundlegend umgestaltet oder erweitert und der Vorschrift damit einen neuen Inhalt oder eine andere Bedeutung gibt oder wenn durch die Gesetzesänderung durch die Einbettung einer äußerlich unverändert gebliebenen Norm in ein anderes gesetzliches Umfeld eine neue und zusätzliche Beschwer geschaffen wird,

> BVerfGE 11, 351 (359 f.); BVerfGE 74, 69 (73); BVerfGE 78, 350 (356); BVerfGE 100, 313 (356); BVerfGE 111, 382 (411); BVerfGE 120, 274 (298); BVerfGE 131, 316 (333); siehe auch *Hömig*, in Maunz/Schmidt-Bleibtreu/Klein/Bethge, BVerfGG, 56. EL Feb 2019, § 93, Rn. 85.

So liegt es hier. Das HVSG ist bei gleichzeitiger Aufhebung des bisherigen Gesetzes komplett novelliert und neu verkündet worden (§ 29 HVSG). Bereits damit wäre die Frist zu einer verfassungsgerichtlichen Überprüfung erneut eröffnet. Darüber hinaus sind die angegriffenen Überwachungsermächtigungen als eigenständige Normen ausgestaltet und in ihrem Anwendungsbereich neu bestimmt worden. Auch die Regelungen zur Datenübermittlung sind komplett neu formuliert worden und in der materiellen Reichweite verändert worden. Soweit die Befugnisse zur Datenübermittlung an ausländische Stellen einen ähnlichen Wortlaut zur Vorgängerregelung aufweisen ergibt sich das veränderte materielle Gewicht aus dem veränderten Gesetzesumfeld, insbesondere daraus, dass die zu übermittelnden Daten aus neuen Ermächtigungsgrundlagen zur Datenerhebung stammen. Die Vorgaben zur Datenverarbeitung sind neu gefasst worden. Die jeweiligen Benachrichtigungspflichten und der Auskunftsanspruch sind ebenfalls überarbeitet und mit neuen Beschränkungen versehen worden. Auch diese Regelungen sind zudem im veränderten Gesetzesumfeld, insbesondere im Zusammenhang mit den überarbeiteten jeweiligen Überwachungsermächtigungen zu betrachten.

Die angegriffenen Regelungen im HSOG stellen materielle Rechtsveränderungen mit neuer und zusätzlicher Beschwer dar. §§ 15c, 25a HSOG sind neu geschaffen worden, in § 15b HSOG ist die Eingriffsschwelle abgesenkt worden.

Die angegriffenen Eingriffsermächtigungen sind gemäß Artikel 5 des Gesetzes zur Neuausrichtung des Verfassungsschutzes in Hessen am Tag nach der Verkündung und damit am 4. Juli 2018 um 00:00 Uhr in Kraft getreten. Die Jahresfrist läuft am 03. Juli 2019 um 23:59 Uhr ab.

II. Beschwerdefähigkeit

Die Beschwerdeführer*innen sind auch beschwerdefähig im Sinne des § 90 Abs. 1 S. 1 BVerfGG. Beschwerdefähig ist demzufolge „jedermann", soweit er fähig ist, Träger von Grundrechten zu sein. Die prozessuale Beschwerdefähigkeit knüpft dabei an die materielle Grundrechtsfähigkeit an,

> BVerfGE 115, 205 (227).

Grundrechtsfähig ist insbesondere auch die Beschwerdeführerin zu 7, bei der es sich nicht um eine natürliche Person handelt. Die Beschwerdeführerin zu 7 rügt eine Verletzung des Grundrechts auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme (dazu unter 1). Die Beschwerdeführerin zu 7 ist fähig, Trägerin dieses Grundrechts zu sein (dazu unter 2).

1. Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme

Die Vertraulichkeit und Integrität informationstechnischer Systeme, auf welche die Beschwerdeführer*innen in besonderem Maße angewiesen sind, ist grundrechtlich geschützt. Dieses Grundrecht der einzelnen Person leitet sich nach der Rechtsprechung des Bundesverfassungsgerichts aus dem Allgemeinen Persönlichkeitsrecht ab (Art. 2 Abs. 1 i.V. mit Art. 1 Abs. 1 GG),

> dazu grundlegend BVerfGE 120, 274 (302 ff.).

Geschützt von diesem Grundrecht ist zunächst das Interesse der Nutzer*innen, dass die von einem vom Schutzbereich erfassten informationstechnischen System erzeugten, verarbeiteten und gespeicherten Daten vertraulich bleiben. Ein Eingriff in dieses Grundrecht ist zudem dann anzunehmen, wenn die Integrität des geschützten informationstechnischen Systems angetastet wird, indem auf das System so zugegriffen wird, dass dessen Leistungen, Funktionen und Speicherinhalte durch Dritte genutzt werden können; dann ist die entscheidende technische Hürde für eine Ausspähung, Überwachung oder Manipulation des Systems genommen,

> BVerfGE 120, 274 (314).

2. Anwendbarkeit auf die Beschwerdeführerin zu 7

Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität von informationstechnischen Systemen steht, soweit es auf Art. 2 Abs. 1 GG gestützt ist, auch der Beschwerdeführerin zu 7 als inländische juristische Personen zu. Denn es ist seinem Wesen nach auch auf sie anwendbar (Art. 19 Abs. 3 GG). Damit ist auch die Beschwerdeführerin zu 7 grundrechts- und beschwerdefähig. Es hängt von Schutzgehalt und Eigenart von Grundrechten ab, ob sie auch auf eine inländische juristische Person anwendbar sind,

> vgl. dazu BVerfGE 95, 220 (242); BVerfGE 106, 28 (42). Ausführlich und m.w.N. siehe *Remmert*, in: Maunz/Dürig, GG, 84. EL Aug. 2018, Art. 19 Abs. 3, Rn. 100.

Zwar leitet sich das IT-Grundrecht aus dem Allgemeinen Persönlichkeitsrecht ab und hat damit eine normative Grundlage auch im Prinzip der Menschenwürde (Art. 1 Abs. 1 GG). Die Gewährleistungen der Menschenwürde sind jedoch, das ist unstreitig, nur anwendbar, soweit ein Grundrecht die psychische oder physische Existenz eines Menschen voraussetzt oder an andere Merkmale und Qualitäten anknüpft, die ein Menschsein voraussetzen,

> vgl. dazu etwa BVerfGE 95, 220 (242); 118, 168 (203).

Auch in Fällen, in welchen die spezifische, grundrechtlich geschützte Freiheitsausübung jedoch keinen derartigen Bezug zur Menschenwürde aufweist, ist der Schutz des Allgemeinen

Persönlichkeitsrechts – und gleichermaßen auch des IT-Grundrechts – auf juristische Personen übertragbar. Denn einzelne Ausprägungen des Allgemeinen Persönlichkeitsrechts können auch korporativ betätigt werden. So hat das Bundesverfassungsgericht festgestellt, dass das Recht auf informationelle Selbstbestimmung, ebenfalls eine Ausprägung des allgemeinen Persönlichkeitsrechts, auch auf juristische Personen anwendbar ist. Das hat es damit begründet, dass juristische Personen hinsichtlich informationeller Maßnahmen des Staates ein Schutzbedürfnis haben, welches dem natürlicher Personen entspräche,

BVerfGE 118, 168 (203).

Unterschiede können sich bei den konkreten Gewährleistungen des Grundrechts ergeben. Denn eine juristische Person, anders als eine natürliche, hat in der Regel einen durch eine bestimmte Zwecksetzung begrenzten Tätigkeitskreis,

BVerfGE 118, 168 (203).

Die Anwendbarkeit des IT-Grundrechts auf juristische Personen ist bislang verfassungsgerichtlich noch nicht entschieden worden. Da es sich ebenfalls um eine Ausprägung des Allgemeinen Persönlichkeitsrechts handelt, lassen sich die bisher etablierten Grundsätze aber übertragen. Soweit sich das IT-Grundrechts auch auf Art. 2 Abs. 1 GG stützt, kann auch eine juristische Person Trägerin dieses Grundrechts sein. Auch für juristische Personen besteht ein besonderes Schutzbedürfnis auf Gewährleistung der Vertraulichkeit von IT-Systemen. Die dort gespeicherten Daten lassen, sollte eine unbefugte Person Zugriff haben, weitreichende Rückschlüsse über die Arbeitsweise, Umsätze, Strategien und Kunden der juristischen Person zu. Die Gefahr eines solchen Zugriffs kann auch für juristische Personen in der Ausübung ihrer grundrechtlichen Freiheiten einschüchternd wirken. Das besondere Schutzbedürfnis, welchem das IT-Grundrecht gerecht wird, knüpft damit nicht an eine Qualität an, die nur Menschen eigen ist.

III. Beschwerdebefugnis

Die Beschwerdeführer*innen sind im Sinne von § 90 Abs. 1 BVerfGG beschwerdebefugt, weil eine Verletzung ihrer Grundrechte durch die von ihnen jeweils angegriffenen Regelungen zumindest möglich ist und diese Regelungen sie auch selbst, gegenwärtig und unmittelbar betreffen. Die Beschwerdeführer*innen zu 1 bis 5 wenden sich gegen alle angegriffenen Regelungen, die Beschwerdeführer zu 6 und 7 gegen die Ermächtigungen zur Quellen-TKÜ und Online-Durchsuchung in §§ 15b, 15c HSOG. Insoweit sind sie jeweils beschwerdebefugt.

1. Beschwerdebefugnis der Beschwerdeführer*innen zu 1-5 in Bezug auf die gerügten Neuregelungen im HVSG und § 25a HSOG

a) Grundrechtsrügen

Die Beschwerdeführer*innen zu 1 bis 5 rügen folgende Grundrechtsverletzungen:
Die angegriffenen Ermächtigungsgrundlagen zur Ortung von Mobilfunkendgeräten gemäß § 9 Abs. 1 HVSG, zur Einholung von Auskünften von Verkehrsunternehmen in § 10 Abs. 2 Nr. 1 HVSG sowie zum Einsatz von verdeckten Mitarbeiter*innen und Vertrauensleuten in §§ 12

Abs. 1, 13 HVSG verletzen die Beschwerdeführer*innen in ihrem allgemeinen Persönlichkeitsrecht in seinen Ausprägungen als Grundrecht auf informationelle Selbstbestimmung, als Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme und als Recht am eigenen Wort und als Recht am eigenen Bild,
(Art. 2 Abs. 1 i.V mit Art. 1 Abs. 1 GG) und ihrem Wohnungsgrundrecht (Art. 13 Abs. 1 GG)

Neben den materiellen Eingriffsvoraussetzungen der genannten Überwachungsermächtigungen rügt die Beschwerde zudem in Bezug auf alle Überwachungsermächtigungen die Verfahrensregelungen zur Schaffung von Transparenz und effektivem Rechtsschutz. Die Ermächtigungen zum Einsatz von Verdeckten Mitarbeitern (§ 12 HVSG) und Vertrauensleuten (§ 13 HVSG) sowie die Ermächtigung zur Ortung von Mobilfunkendgeräten (§ 9 HVSG) sehen eine Benachrichtigung überhaupt nicht vor und sind schon deshalb sowohl im Lichte der genannten, durch sie tangierten Grundrechte als auch unter dem Gesichtspunkt effektiven Rechtsschutzes im Sinne des Art. 19 Abs. 4 GG mangelhaft. Die Benachrichtigungspflichten in §§ 6 Satz 5, 8 Abs. 4, 10 Abs. 6, 11 Abs. 9 sowie der in § 26 HVSG enthaltene Auskunftsanspruch unterliegen zu weitreichenden Beschränkungen und verletzen die Beschwerdeführer*innen zu 1-5 so in ihrem Grundrecht auf individuellen Rechtsschutz (Art. 19 Abs. 4 GG). Zudem führen die unzureichenden Transparenzregelungen in Verbindung mit den jeweiligen Überwachungsermächtigungen zu einer Verletzung des Grundrechts der Beschwerdeführer*innen auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V. mit Art. 1 Abs. 1 GG), ihrem Telekommunikationsgeheimnis (Art. 10 Abs. 1 GG) und ihrem Wohnungsgrundrecht (Art. 13 Abs. 1 GG).

Die in §§ 16, 20 Abs. 1 Nr. 1 und 2, Abs. 2 Satz 1 Nr. 2, Abs. 2 Satz 2, 21 Abs. 2 HVSG enthaltenen Ermächtigungen zur Datenverarbeitung und Datenübermittlung reichen zu weit und verletzen deshalb die Beschwerdeführer*innen zu 1-5 in ihrem Grundrecht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V. mit Art. 1 Abs. 1 GG), ihrem Telekommunikationsgeheimnis (Art. 10 Abs. 1 GG), ihrem Wohnungsgrundrecht (Art. 13 Abs. 1 GG) und ihrem Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (Art. 2 Abs. 1 i.V. mit Art. 1 Abs. 1 GG bzw. Art. 2 Abs. 1 GG).

Die Ermächtigung zur automatisierten Datenanalyse gemäß § 25a HSOG verletzt die Beschwerdeführer*innen zu 1-5 in ihrem Grundrecht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V. mit Art. 1 Abs. 1 GG) und, soweit Daten aus der Wohnraumüberwachung, der Telekommunikationsüberwachung oder der Online-Durchsuchung analysiert werden, auch in ihrem Wohnungsgrundrecht (Art. 13 Abs. 1 GG), ihrem Telekommunikationsgeheimnis (Art. 10 Abs. 1 GG) und ihrem Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (Art. 2 Abs. 1 i.V. mit Art. 1 Abs. 1 GG bzw. Art. 2 Abs. 1 GG).

b) Eigene und gegenwärtige Beschwer

(1) In Bezug auf die angegriffenen Regelungen im HVSG

Die Beschwerdeführer*innen zu 1-5 sind durch die angegriffenen Regelungen im HVSG selbst und gegenwärtig betroffen. Erforderlich, aber auch ausreichend für die Darlegung einer

eigenen Betroffenheit ist bei Verfassungsbeschwerden gegen Ermächtigungen zu gegen einzelne Personen gerichteten verdeckten Überwachungen und zum Umgang mit den dadurch erlangten personenbezogenen Daten, dass der Beschwerdeführer aufgrund seines Vortrags mit hinreichender Wahrscheinlichkeit als Zielperson oder Dritter von einer Überwachungsmaßnahme betroffen sein kann,

> vgl. BVerfGE 141, 220 (262), stRspr.

Dies ist für die Beschwerdeführer*innen zu 1 bis 5 zu bejahen.
Die Beschwerdeführer*innen 1 und 2 nehmen Führungsrollen in einer Organisation ein, die das Landesamt als extremistisch einstuft und deshalb beobachtet. Über sie hat das Landesamt zudem nachweislich bereits eine Vielzahl von Informationen zusammengetragen. Die Sperrerklärung des Beklagten im Verwaltungsgerichtsverfahren der Beschwerdeführerin zu 1 deutet zudem darauf hin, dass dies auch unter Einsatz verdeckter Ermittler und von Vertrauenspersonen geschah. Das Landesamt hat im Rahmen dieses Verfahrens zudem mehrfach deutlich gemacht, dass die Klägerin im Kontext ihrer Aktivitäten für nach Auffassung des Landesamtes extremistisch beeinflusste und extremistische Organisationen auch weiterhin beobachtet werde,

> VG Kassel, Urteil vom 15.10.2017, Az. 4K641/13.KS, S. 7 ff.

Für die Beschwerdeführer*innen zu 1 und 2 besteht nicht nur in Bezug auf ihre eigene Person ein beträchtliches Risiko, von Überwachung betroffen zu sein, sondern sie laufen auch Gefahr im Rahmen ihrer politischen Tätigkeit von Überwachungen betroffen zu werden, die sich gegen andere Organisationen oder einzelne ihrer Mitglieder richten. Die Beschwerdeführer*innen zu 1 und 2 stehen regelmäßig mit weiteren Mitgliedern und Unterstützer*innen der VVN-BdA, als auch mit Mitgliedern und Unterstützer*innen weiterer Organisationen in Verbindung, die das Landesamt als linksextremistisch einstuft, in Kontakt. Beispielhaft sei die DKP genannt. Neben dem Einsatz von Vertrauenspersonen und verdeckten Ermittlern können die Beschwerdeführer*innen zu 1 und 2 im Rahmen ihrer Beobachtung durch das Landesamt auch mit hinreichender Wahrscheinlichkeit von einer Auskunft bei Verkehrsunternehmen oder einer Ortung ihres Mobilfunkendgerätes betroffen sein. Ihnen und ihrem Umfeld werden Bestrebungen und Tätigkeiten nach § 2 Abs. 2 HVSG vorgeworfen. Die darüberhinausgehende Darlegung einer von ihnen ausgehenden gegenwärtigen schwerwiegenden Gefahr für die Schutzgüter des § 2 Abs. 2 HVSG ist nicht zumutbar oder erforderlich,

> BVerfGE 133, 277 (312).

Auch die Beschwerdeführer*innen zu 3 und 4 sind von den Neuregelungen im HVSG selbst und gegenwärtig betroffen. Viele ihrer Mandant*innen werden vom Landesamt beobachtet, sei es weil ihnen die Mitgliedschaft in ausländischen terroristischen Vereinigungen vorgeworfen wird oder weil sie der linksextremistischen Szene zugeordnet werden.

Die Betroffenheit der Beschwerdeführer*innen zu 3 und 4 wird insoweit auch nicht durch die Erhebungs- und Verwertungsverbote, die aus Berufsgeheimnissen folgen, in Frage gestellt. Diese können eine ansonsten gegebene Betroffenheit von einer Eingriffsermächtigung richtigerweise nicht beseitigen. Sonst würde der privilegierende Schutzzweck der Berufsgeheimnisse konterkariert. Die Berufsgeheimnisse sollen den Berufsträgern einen stärkeren Schutz verleihen, nicht ihren ansonsten bestehenden grundrechtlichen Schutz schwächen.

Die sonstigen Eingriffsvoraussetzungen dienen insoweit erst recht ebenso dem Schutz des Berufsträgers. Wo eine Betroffenheit ansonsten greift und nur vom Berufsgeheimnis als Gegenausnahme in Frage gestellt wird, kann die Betroffenheit und das daraus folgende prozessuale Recht, auch die Einhaltung der sonstigen Eingriffsvoraussetzungen gerichtlich zur Prüfung zu stellen, nicht ausgerechnet wegen des auf Privilegierung zielenden Berufsgeheimnisses entfallen. Wo schon die nicht privilegierte Person klagen kann, muss erst recht auch der Berufsgeheimnisträger klagen können.

Zudem bleibt es außerhalb der Reichweite dieser Schutzbestimmungen bei der persönlichen Betroffenheit. Schließlich kann auch dann, wenn etwa die Geltung des Erhebungsverbotes erst im Laufe einer Überwachungsmaßnahme festgestellt wird, der Beobachtende schon aus den, bis dahin erlangten Informationen, etwa den ersten Sätzen eines Gesprächs, gegebenenfalls weiterführende Schlüsse ziehen. Die Überwachung des dienstlichen Mobiltelefons des Beschwerdeführers zu 4 zeigt zudem, dass der Schutz des Berufsgeheimnisses mitunter missachtet wird und die Kommunikation mit Mandant*innen gleichwohl überwacht wird. Auch beim Einsatz von Vertrauensleuten und verdeckten Mitarbeiter*innen kann nicht gewährleistet werden, dass vertrauliche Informationen aus dem Mandatsverhältnis nicht erhoben werden. In vielen Situationen wird die Aufrechterhaltung der Legende der Unterbrechung entsprechender Gespräche entgegenstehen.

Auch der Beschwerdeführer zu 5 ist von den Neuregelungen im HVSG betroffen. Er berichtet häufig über politisch „links" ausgerichtete Gruppierungen und steht im Rahmen seines ehrenamtlichen politischen Engagements mit politischen Aktivist*innen und Organisationen, die vom Verfassungsschutz beobachtet werden, im Kontakt. Diese Kontakte bergen die Gefahr, als Beifang von Überwachungsmaßnahmen durch das Landesamt betroffen zu sein.

Weitere Darlegungen sind den Beschwerdeführer*innen zu 1-5 weder möglich noch zumutbar. Die konkreten Überwachungsmaßnahmen des Landesamts sind ihnen nicht bekannt. Im Verwaltungsgerichtsverfahren der Beschwerdeführerin zu 1 auf Auskunft über die durch das Landesamt erhobenen personenbezogenen Daten und Einstellung der weiteren Beobachtung ist deutlich geworden, dass weitere Informationen über bisherigen und künftige Überwachungsmaßnahmen und die erhobenen Daten nicht zu erlangen sind,

> VG Kassel, Urteil vom 15.10.2017, Az. 4K641/13.KS, S. 2.

Bereits auf der Grundlage der bisherigen Ausführungen ist die Wahrscheinlichkeit, dass die Beschwerdeführer*innen 1-5 von Überwachungsmaßnahmen des Landesamts als Zielpersonen oder Dritte betroffen werden könnten, im Vergleich zum Bevölkerungsdurchschnitt weit erhöht.

(2) In Bezug auf die automatisierte Datenanalyse, § 25a HSOG

Die Beschwerdeführer*innen zu 1-5 sind auch selbst und gegenwärtig durch die automatisierte Datenanalyse gemäß § 25a HSOG beschwert. Sie werden mit einiger Wahrscheinlichkeit durch die automatisierte Datenanalyse in ihren Grundrechten berührt,

> vgl. zu diesem Erfordernis BVerfGE 109, 279 (307 f.); s. auch BVerfGE141, 220 (262) („mit hinreichender Wahrscheinlichkeit").

Die eigene und gegenwärtige Betroffenheit der Beschwerdeführer*innen zu 1-5 folgt aus der Weite des Adressatenkreises der Ermächtigung. Für den geforderten Grad der Wahrscheinlichkeit ist bedeutsam, ob die angegriffene Maßnahme auf einen tatbestandlich eng umgrenzten Personenkreis zielt oder eine große Streubreite hat und Dritte auch zufällig erfassen kann,

> vgl. BVerfGE 109, 279 (307 f.).

Durch den Einsatz zur vorbeugenden Bekämpfung von Straftaten nach § 100a Abs. 2 StPO greift die automatisierte Datenanalyse schon in Bezug auf die unmittelbaren Zielpersonen im Vorfeld einer konkreten Gefahr. Für die vorbeugende Straftatbekämpfung reichen schon abstrakte Gefahrenlagen,

> vgl. Denninger, in: Lisken/ders. (Hrsg.), Handbuch des Polizeirechts, 5. Aufl. 2012, Rn. D 1 ff., m.w.N. Dieses Verständnis tritt auch in der Gesetzesbegründung zu § 25a HSOG zutage, wonach die Datenanalyse überhaupt erst der Gewinnung wesentlicher Anhaltspunkte für Gefahren und bevorstehende Straftaten dient, Hessischer Landtag, Drs. 19/6502, Seite 41.

Zudem finden sich in dem Straftatkatalog des § 100a StPO neben Erfolgsdelikten auch Gefährdungstatbestände wie die §§ 129-130 StGB, die Handlungen im Vorfeld einer Rechtsgutsverletzung kriminalisieren, und auf deren Grundlage in der Vergangenheit immer wieder auch in linksextremistischen Strukturen ermittelt wurde,

> exemplarisch ist das mittlerweile eingestellte Ermittlungsverfahren der Staatsanwaltschaft Dresden gegen ca. 50 Menschen einer sogenannten „Antifa-Sportsgruppe" wegen Bildung einer kriminellen Vereinigung nach § 129 StGB, aufgrund dessen zwischen 2010 und 2014 offene und verdeckte Observationen, Telefon- und Internetüberwachungen, Hausdurchsuchungen, Beschlagnahmungen von Computern und persönlichen Sachen, Funkzellenabfragen und weitere Überwachungsmaßnahmen stattfanden, https://www.dka-kanzlei.de/news-reader/erstes-129-verfahren-gegen-antifaschistinnen-in-dresden-eingestellt.html, zuletzt abgerufen am 01.07.2019.

Nimmt man die von der automatisierten Datenanalyse auch unvermeidlich betroffenen Dritten oder im Zusammenhang mit der Zielperson stehenden Personen hinzu, ergibt sich eine so hohe Streubreite der Eingriffe, dass die Beschwerdeführer*innen zu 1-5 deutlich mit hinreichender Wahrscheinlichkeit von diesen Maßnahmen betroffen sein können.

Schließlich soll die automatisierte Datenanalyse Erkenntnisse über „gemeinsame Strukturen, Handlungsmuster, Personengruppen und zeitliche, sachliche, organisatorische, personale und situative Zusammenhänge" bringen,

> LT- Drs. 19/6502, Seite 41.

Mithin bezieht die Analyse nicht nur Daten der unmittelbaren Zielperson ein, sondern auch Daten von Menschen aus dem Umfeld der Zielperson und darüber hinaus auch von vollkommen unbeteiligten Menschen, die beispielsweise mit einem Ort oder einem Ereignis in Verbindung stehen. Schließlich kann jede Beziehung eines Objekts mit einem anderen Objekt zur Auswertung herangezogen werden und dies führt zu weiteren Objekten, die wieder mit anderen Objekten in Beziehung stehen. Diese Form der Analyse kann buchstäblich jeden treffen,

bei Berücksichtigung von Melderegister oder Fahrzeughalterdaten auch Menschen, die noch nie anlassbezogen, polizeilich erfasst wurden.
Die Beschwerdeführer*innen zu 1-5 sind aufgrund ihrer „politischen, beruflichen und privaten Verbindungen zu potenziellen Zielpersonen" von den angegriffenen Maßnahmen mit hinreichender Wahrscheinlichkeit betroffen,

> vgl. BVerfGE 141, 220 (262). Siehe auch BVerfGE 109, 279 (307 f.); 113, 348 (363 f.); 133, 277 (312 f.).

Die Beschwerdeführer*innen zu 1und 2 sind selbst in einer als verfassungsfeindlich eingestuften Organisation Mitglied und stehen regelmäßig mit entsprechenden Organisationen und ihren Mitgliedern im Kontakt. Beim Verfassungsschutz existieren zahlreiche personenbezogene Daten der Beschwerdeführer*innen zu 1 und 2. Ob in Polizeidatenbanken Informationen über die Beschwerdeführer*innen zu 1 und 2 gespeichert sind, ist nicht bekannt, jedoch aufgrund der politischen Tätigkeit durchaus wahrscheinlich. Zudem kann das Landesamt die Daten bei Bedarf gemäß § 20 Abs. 2 HVSG an die Hessische Polizei übermitteln.

Insofern besteht eine hinreichende Wahrscheinlichkeit, dass im Zuge einer Datenanalyse einer Zielperson aus dem „linksextremistischen" Umfeld auch die Daten der Beschwerdeführer*innen zu 1 und 2 als Beifang angezeigt werden. Dafür reicht unter Umständen schon eine Mailkommunikation mit der Zielperson, der Besuch der gleichen Veranstaltung oder die Nummer im Mobiltelefon der Zielperson.

Die Beschwerdeführerin zu 3 vertritt zahlreiche Mandant*innen, denen die Mitgliedschaft in ausländischen terroristischen Vereinigungen vorgeworfen wird. Diese Personen werden in zahlreichen Polizeidatenbanken geführt, beispielsweise als sogenannte Gefährder oder aufgrund der gegen sie geführten Ermittlungs- und Strafverfahren. Da die Beschwerdeführerin zu 3 regelmäßig mit ihren Mandant*innen kommuniziert und diese auch trifft, ist es auch in ihrem Fall wahrscheinlich, dass ihre personenbezogenen Daten im Rahmen der automatisierten Datenanalyse angezeigt werden. Der mutmaßliche Missbrauch der personenbezogenen Daten der Beschwerdeführerin zu 3 durch die hessische Polizei verdeutlicht, welche Gefahr darin liegt, dass bei der Polizei Datenbestände wie Melderegisterauszüge zu jedermann gespeichert sind und dort von beliebigen Polizisten abgerufen und mit anderen Datenbestände ausgewertet werden können.

Die Beschwerdeführer zu 4 und 5 sind selbst politisch aktiv und stehen im Rahmen ihrer beruflichen Tätigkeit als Anwalt bzw. Journalist ebenso wie im Rahmen ihrer privaten politischen Engagements regelmäßig mit politischen Aktivist*innen und als extremistisch eingestuften Organisationen im Kontakt. Aufgrund dieser Kontakte besteht auch für die Beschwerdeführer zu 4 und 5 eine erhöhte Wahrscheinlichkeit, Beifang einer automatisierten Datenanalyse durch die Polizei Hessen zu sein.

Weitere Darlegungen sind den Beschwerdeführer*innen zu 1-5 weder möglich noch zumutbar. Insbesondere kann zum Beleg der eigenen gegenwärtigen Betroffenheit nicht verlangt werden, dass sich die Beschwerdeführer*innen selbst einer Straftat oder als möglicher Verursacher einer Gefahr für die öffentliche Sicherheit bezichtigen,

> BVerfGE 133, 277 (312).

c) Unmittelbare Beschwer

Schließlich sind die Beschwerdeführer*innen durch die angegriffenen Regelungen unmittelbar betroffen. Zwar bedürfen die Ermächtigungen der behördlichen Umsetzung. Von einer unmittelbaren Betroffenheit durch ein Gesetz ist jedoch auch dann auszugehen, wenn Beschwerdeführer*innen den Rechtsweg nicht beschreiten können, weil sie keine Kenntnis von der betreffenden Vollziehungsmaßnahme erhalten. In solchen Fällen steht ihnen die Verfassungsbeschwerde unmittelbar gegen das Gesetz zu,

> BVerfGE 133, 277 (311); 141, 220 (261).

So liegt es hier: Die in den angegriffenen Regelungen geregelten Überwachungsmaßnahmen, Datenverarbeitungen, Datenübermittlungen und Datenanalysen werden verdeckt durchgeführt. In Bezug auf die automatisierte Datenanalyse sieht das HSOG keine Benachrichtigungspflichten vor. Die im HVSG vorgesehenen Pflichten des Landesamts zur Benachrichtigung der Betroffenen fangen den verdeckten Charakter der Eingriffe nur unzureichend auf, weil sie nicht alle Überwachungsmaßnahmen erfassen, möglicherweise erst spät greifen und weitreichende Ausnahmen kennen. Die Ermächtigungen zum Einsatz von Verdeckten Mitarbeiter*innen (§ 12 HVSG) und Vertrauensleuten (§ 13 HVSG), die Ermächtigung zur Ortung von Mobilfunkendgeräten (§ 9 HVSG) sehen eine Benachrichtigung überhaupt nicht vor.

Soweit das HVSG eine Benachrichtigung des Betroffenen vorsieht (§§ 6 S. 5, 10 Abs. 6, 8 Abs. 4, 11 Abs. 9 HVSG) enthalten die Regelungen sehr weit gefasste Ausnahmen. So unterbleibt die Benachrichtigung, solange eine Gefährdung des Zwecks der Beschränkung nicht ausgeschlossen werden kann oder wenn übergreifende Nachteile für das Wohl des Bundes oder eines Landes absehbar sind. Von der Übermittlung personenbezogener Daten erhalten die Betroffenen in aller Regel keine Kenntnis. Der in Art. 26 HVSG enthaltene Auskunftsanspruch enthält gleichfalls weitreichende Ausnahmetatbestände, so dass Personen, die von Überwachungsmaßnahmen und Datenübermittlungen betroffen sind, auch mit seiner Hilfe nicht durchweg einen effektiven Rechtsschutz erlangen können. Besonders eindrücklich veranschaulicht dies der Fall der Beschwerdeführerin zu 1, deren Personenakte im Verwaltungsverfahren nur mit umfassenden Schwärzungen und Sperrvermerken offengelegt wurde. Welchen Überwachungsmaßnahmen die Beschwerdeführerin zu 1 ausgesetzt war, konnte sie nicht erkennen, ebenso wenig, ob Daten an andere öffentliche Stellen übermittelt wurden,

> vgl. Sperrerklärung des Landesamts für Verfassungsschutz Hessen nach § 99 Abs. 1 Satz 2 VwGO vom 07.10.2013.

2. Beschwerdebefugnis der Beschwerdeführer*innen 1-7 in Bezug auf die Quellen-TKÜ und Online-Durchsuchung in §§ 15b, 15c HSOG

In Bezug auf §§ 15b, 15c HSOG rügen die Beschwerdeführer*innen zu 1 bis 7 die Verletzung ihres Rechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (Art. 2 Abs. 1 i.V. mit Art. 1 Abs. 1 GG bzw. Art. 2 Abs. 1 GG). Die Beschwerdeführer*innen sind in herausgehobener Weise auf die Vertraulichkeit ihrer IT-Systeme angewiesen, dies jeweils auch zum Schutz der Rechte anderer Menschen. Die mögliche Verletzung ihres Rechts auf Gewährleistung dieser Vertraulichkeit liegt darin, dass das Land Hessen durch die Einführung der angegriffenen Rechtsgrundlagen in §§ 15b, 15c HSOG ohne eine

flankierende Regelungen des Umgangs mit IT-Schwachstellen einen Anreiz dafür setzt, dass staatliche Behörden die IT-Sicherheit der Beschwerdeführer*innen zusätzlich gefährden. Denn für Gefahrenabwehrbehörden in Hessen ist es aufgrund dieser Regelung zukünftig von Vorteil, IT-Schwachstellen geheim zu halten, um sie somit möglichst lange für Online-Durchsuchung und Quellen-TKÜ ausnutzen zu können, statt sie den Herstellern zu melden und ihr Beheben zu ermöglichen (dazu unter a). Der Grundrechtschutz der Gewährleistung der Vertraulichkeit von IT-Systemen beinhaltet dem hingegen die staatliche Pflicht, sich für IT-Sicherheit einzusetzen und damit schützend vor dieses Recht zu stellen (dazu unter b). Aufgabe des Staates ist es insofern, sicherzustellen, dass staatliche Stellen auf die Behebung von Schwachstellen in der IT-Sicherheit hinwirken (dazu unter c). Aufgrund ihrer jeweiligen beruflichen und privaten Tätigkeit sind die Beschwerdeführer zu 1-7 in besonderem Maße darauf angewiesen, dass die Vertraulichkeit ihrer IT-Systeme gewährleistet ist und Sicherheitslücken behoben werden, und deshalb zumindest möglicherweise betroffen. (dazu unter d). Sie sind auch selbst, gegenwärtig und unmittelbar betroffen (dazu unter e).

a) Herausgehobene Rolle von Schwachstellen-Exploits bei der Umsetzung von Quellen-TKÜ

Das Ausnutzen von Schwachstellen spielt mutmaßlich bei der Umsetzung von Online-Durchsuchung und Quellen-TKÜ durch die Polizei Hessen eine große Rolle. Diese Form des Eindringens in ein IT-System hat nämlich gegenüber den möglichen Alternativen deutliche, praktische Vorteile, da weder ein räumlicher Zugriff noch ein weiteres Fehlverhalten eines*r Nutzer*in notwendig ist. Gerade wegen dieses strategischen Vorteils werden solche Schwachstellen auf dem Schwarzmarkt für hohe Summen gehandelt,

> vgl. dazu *Kai Biermann*, Außenministerium will Internet sicherer machen, BND nicht, die ZEIT vom 9. Oktober 2017, online abrufbar unter: https://www.zeit.de/digital/datenschutz/2017-10/it-sicherheit-bnd-zero-day-aussenministerium, zuletzt abgerufen am 01.07.2019.

Auf Bundesebene gab der Abteilungsleiter für Cyber- und IT-Sicherheit im Bundesministerium des Inneren und für Bauen und Heimat, Andreas Könen, zu, dass der Entwicklungs- und Beschaffungsprozess für Trojaner, welche gerade Schwachstellen ausnutzen, in Gang gesetzt wurde,

> es handele sich derzeit, so seine Aussage aus dem Juni 2018, um höchstens 5 Prozent des Zugriffs. *Detlef Borchers*, Cyber-Sicherheitspolitik: Fünf Prozent Zero-Day-Lücken für staatliche Überwachung von Kriminellen, Heise-Online vom 6. Juni 2018, online abrufbar unter: https://www.heise.de/newsticker/meldung/Cyber-Sicherheitspolitik-Fuenf-Prozent-Zero-Day-Luecken-fuer-staatliche-Ueberwachung-von-Kriminellen-4072578.html, zuletzt abgerufen am 01.07.2019.

Die vom Bundeskriminalamt entwickelten und angekauften Trojaner setzen denn ebenfalls, soweit bekannt, vollständig oder überwiegend auf das Ausnutzen von Sicherheitslücken.

Für eine Liste der verfügbaren Trojaner siehe *Andre Meister*, Geheime Dokumente: Das Bundeskriminalamt kann jetzt drei Staatstrojaner einsetzen, Netzpolitik.org vom 26. Juni 2018, online abrufbar unter: https://netzpolitik.org/2018/geheime-dokumente-das-bundeskriminalamt-kann-jetzt-drei-staatstrojaner-einsetzen/, zuletzt abgerufen am 01.07.2019.

Es ist deshalb mit hoher Wahrscheinlichkeit davon auszugehen, dass auch die Polizeibehörden Hessen Online-Durchsuchung und Quellen-TKÜ gerade unter Ausnutzung von IT-Sicherheitslücken durchführen werden.

b) Schutzdimension des IT-Grundrechts

Neben der Abwehrdimension leiten sich aus Art. 2 Abs. 1 i.V. mit Art. 1 Abs. 1 GG bzw. Art. 2 Abs. 1 auch grundrechtliche Schutzpflichten für die Gewährleistung der Integrität und Vertraulichkeit von informationstechnischen Systemen ab,

vgl. allgemein zu Schutzpflichten bzgl. des Allgemeinen Persönlichkeitsrechts *Di Fabio*, in: Maunz/Dürig, GG, Stand: 81. EL Sep. 2017, Art. 2 Rn. 135 f.

Das Grundrecht verbürgt nämlich auch den staatlichen Auftrag zur **Gewährleistung** der Vertraulichkeit und Integrität informationstechnischer Systeme. Diesen Auftrag erfüllt der Staat, indem er den Einzelnen auch vor Angriffen Dritter auf seine IT-Systeme schützt, in welcher konkreten Form auch immer: Die Beschwerdeführer verkennen nicht, dass dem Gesetzgeber im Bereich der grundrechtlichen Schutzpflichten traditionell ein weiter Gestaltungsspielraum zugebilligt wird. Dieser wird jedoch dann verlassen, wenn das Land Hessen seiner Schutzpflicht überhaupt nicht nachkommt oder sogar, wie vorliegend, gegensätzliche Anreize setzt. Die Vernachlässigung einer solchen grundrechtlichen Schutzpflicht kann von den Betroffenen mit der Verfassungsbeschwerde geltend gemacht werden,

BVerfGE 77, 170 (214); 77, 381 (402 f.); 79, 174 (201 f.); 125, 39 (78).

c) Aufgabe des Landes Hessen bei der Gewährleistung der IT-Sicherheit

Für den Schutz ihrer IT-Systeme hängen die Beschwerdeführer*innen in erster Linie von Maßnahmen der Hersteller der von ihnen verwendeten Programme und IT-Systeme ab. Der Staat spielt jedoch eine wesentliche Rolle in der Herstellung der IT-Sicherheit. Staatliche Stellen können Kenntnis von Sicherheitslücken noch vor den Herstellern der betroffenen Programme und IT-Systeme erhalten, beispielsweise über Meldungen von Firmen oder Behörden, die von Angriffen auf ihre IT-Systeme betroffen waren. Die Möglichkeit zu Maßnahmen nach §§ 15b, 15c HSOG begünstigen indes einen Umgang mit solchen Sicherheitslücken, der sich auf die Beschwerdeführer*innen zu 3-7 in ganz besonderem Maße, abgeschwächt aber auch auf die Beschwerdeführer*innen 1 und 2 und die restliche Bevölkerung fatal auswirkt. Denn durch die Erlaubnis, IT-Sicherheitslücken für Angriffe auf Zielpersonen in der Gefahrenabwehr zu nutzen, schaffen §§ 15b, 15c HSOG einen starken Anreiz für die Polizei und andere staatliche Stellen, Sicherheitslücken gerade nicht den Herstellern zu melden und dadurch zu ihrer Schließung beizutragen. Denn Sicherheitslücken sind im Ankauf teuer und bieten im Zugriff die oben genannten praktischen Vorteile.

Siehe wiederum *Kai Biermann*, Außenministerium will Internet sicherer machen, BND nicht, die ZEIT vom 9. Oktober 2017, online abrufbar unter: https://www.zeit.de/digital/datenschutz/2017-10/it-sicherheit-bnd-zero-day-aussenministerium, zuletzt abgerufen am 01.07.2019.

Damit legen die angegriffenen Normen es – jedenfalls im Zusammenspiel mit dem staatlichen Unterlassen, klare Regeln für das Melden von Sicherheitslücken aufzustellen – den Polizeibehörden Hessens geradezu nahe, möglichst umfangreich staatliche Infiltrationsmöglichkeiten zu sammeln und geheim zu halten, die sich für Maßnahmen nach §§ 15b, 15c HSOG nutzen lassen.
Sachgerecht und naheliegend wäre deshalb etwa eine umfassende Verpflichtung aller staatlicher Stellen, insbesondere aber der mit der Durchführung von Maßnahmen nach §§ 15b, 15c HSOG betrauten Stellen, ihnen bekannte, dem Hersteller aber noch unbekannte Sicherheitslücken diesem zu melden, damit für Abhilfe gesorgt werden kann. Eine solche Pflicht besteht indes nicht. Als absolute Mindestanforderung hat das Land Hessen aber im Lichte seines Schutzauftrags davon abzusehen, eine ohnehin prekäre IT-Sicherheitslage noch zu verschärfen, indem es durch die gesetzliche Neuregelung der §§ 15b, 15c HSOG massive Anreize zum Horten und Geheimhalten von Sicherheitslücken schafft.

Eine staatliche Pflicht zum Schutz der IT-Systeme von Privaten bejahen auch *Roßnagel/Schnabel*, NJW 2008, 3534 (3535); *Becker*, NVwZ 2015, 1335 (1339 f.) *Sachs/Krings*, JuS 2008, 481 (486). Für eine ausführliche Herleitung der Schutz- und Förderpflicht zur Gewährleistung der IT-Sicherheit *Heckmann*, in: FS Käfer, 2009, S. 129 (133 ff.).

d) Besondere Schutzbedürftigkeit der Beschwerdeführer*innen 1-7

Die Beschwerdeführer*innen zu 1-7 sind in besonderem Maße darauf angewiesen, dass – infolge der Fehlbarkeit menschlichen Handelns als solche unvermeidbare – Sicherheitslücken ihrer IT-Systeme schnellstmöglich geschlossen werden. Denn je länger eine Sicherheitslücke besteht, desto höher die Wahrscheinlichkeit, dass sie durch interessierte Kreise gefunden und für Angriffe auf die IT-Systeme der Beschwerdeführer missbraucht wird.

Die Beschwerdeführer*innen zu 1 und 2 kommunizieren regelmäßig mit politisch engagierten Menschen, die Gefahr laufen von ausländischen staatlichen Stellen oder politischen Organisationen überwacht zu werden. Dazu zählen sowohl Sympathisant*innen der PKK als auch Aktivist*innen aus der antifaschistischen oder kommunistischen Szene.

Die Beschwerdeführer*innen zu 3 und 4 bedürfen eines besonderen Schutzniveaus von IT-Systemen und IT-gestützter Kommunikation, um als Rechtsanwälte mit einem bestimmten Kreis von Mandant*innen die Vertraulichkeit der geschützten Kommunikation sicherstellen zu können. Dabei müssen sie sowohl auf ein hohes Schutzniveau der eigenen IT-Systeme als auch auf ein solches Schutzniveau der IT-Systeme ihrer Mandanten vertrauen können. Denn nur, wenn die jeweiligen IT-Systeme und die IT-gestützte Kommunikation sicher vor fremdem Zugriff sind, können sie sicherstellen, dass die in ihrem IT-System gespeicherten, die Mandatsarbeit betreffenden Daten vor fremdem Zugriff geschützt sind und andererseits die Kommunikation mit ihren Mandant*innen vertraulich ist. Und nur bei hinreichend gewährleisteter IT-Sicherheit können sie ihren Mandant*innen auch ein Vertrauen auf die Vertraulichkeit der Mandatsarbeit vermitteln. Gerade Schwachstellen, über welchen ein Zugriff durch Dritte nicht verhindert und kaum bemerkt werden kann, bieten dafür ein Risiko.

Die Vertraulichkeit der Kommunikation ist für jede*n Anwält*in von großer Bedeutung. Bei den Beschwerdeführern zu 3 und 4 kommt jedoch darüber hinaus hinzu, dass ein Teil ihrer Mandant*innen und damit auch sie selbst von einer deutlich erhöhten Wahrscheinlichkeit ausgehen müssen, dass ihre IT-Systeme angegriffen werden. Mehreren der Mandant*innen der Beschwerdeführerin zu 3 wird die Begehung terroristischer Straftaten oder die Mitgliedschaft in ausländischen terroristischen Vereinigungen vorgeworfen. Es ist davon auszugehen, dass diese Personen auch von ausländischen Geheimdiensten überwacht werden. Auch die hochvertrauliche Kommunikation der Beschwerdeführerin zu 3 mit dem betroffenen Mandanten*innen ist von dieser Überwachung betroffen. Der Beschwerdeführer zu 4 betreut überwiegend Mandant*innen aus politischen Kreisen an, in welchen immer wieder Individuen von ausländischen staatlichen Stellen oder politischen Organisationen überwacht werden. Dazu zählen sowohl Sympathisant*innen der PKK als auch Aktivist*innen aus der antifaschistischen oder kommunistischen Szene. Andere Mandant*innen befürchten eine Überwachung ausländischer Geheimdienste aufgrund ihrer beruflichen Tätigkeit oder einer politischen Verfolgung im Heimatland.

Aufgrund dieser Mandatsarbeit müssen die Beschwerdeführer*innen zu 3 und 4 ihren Mandant*innen ein besonderes Maß an Vertraulichkeit zusichern können, und müssen sie zudem selbst befürchten, Ziel von Angriffen auf ihre IT-Systeme zu werden. Zusätzlich haben die Beschwerdeführer zu 3 und 4 auch ein privates Interesse an Datensicherheit, da sie legitimierweise eine eigene Überwachung durch kriminelle oder ausländische staatliche Akteure nicht wünschen.

Der Beschwerdeführer zu 5 ist als investigativ arbeitender Journalist ebenfalls in besonderem Maße auf einen hohen Schutz von IT-Systemen angewiesen, um seine Quellen und auch sich selbst zu schützen.
Informat*innen, beispielsweise Whistleblower, gehen ein hohes Risiko ein, wenn sie Informationen an eine*n Journalist*in weitergeben, um so bestehende Missstände aufzudecken. Um sie und auch sich selbst keiner Gefahr auszusetzen, ist der Beschwerdeführer zu 5 darauf angewiesen, dass organisierte Kriminalität, aber auch ausländische Sicherheitsbehörden nicht auf seine IT-Systeme oder die IT-Systeme seiner Informant*innen zugreifen können. Dafür ist es wichtig, dass die genutzten IT-Systeme vor fremdem Zugriff bestmöglich geschützt sind. Gerade das Schließen von Sicherheitslücken ist dafür wesentlich,

> Peter Welchering/Manfred Kloiber, Informantenschutz, Ethische, rechtliche und technische Praxis in Journalismus und Organisationskommunikation, Springer Wiesbaden 2017, S. V-VII, 105-116.

Gerade die Kommunikation des Beschwerdeführers zu 5 mit regierungskritischen Personen aus Ländern mit repressiven Regierungen ist in besonderem Maße gefährdet, durch die jeweiligen Geheimdienste dieser Länder überwacht zu werden. Auch im Rahmen seines politischen Engagements ist der Beschwerdeführer auf eine sichere Kommunikation angewiesen. Als Vorsitzender der Humanistischen Union Marburg sowie als Ansprechpartner des Arbeitskreises "Psychiatrie" der Humanistischen Union wird der Beschwerdeführer zu 5 immer wieder in sehr persönlichen Angelegenheiten angesprochen, die absolutes Vertrauen und Informantenschutz zwingend erfordern. Aufgrund seiner Blindheit ist er in besonderem Maß auf die Nutzung von sicheren IT-Systemen angewiesen ist und kann nicht auf analoge Aufbewahrungsmöglichkeiten ausweichen.

Auch die Beschwerdeführer*innen zu 6 und 7 sind in besonderem Maße auf einen Schutz ihrer IT-Systeme angewiesen. Der Beschwerdeführer zu 6 vereint in seiner Person Zugriffsrechte auf ungewöhnlich viele sensible Daten. Als Aufsichtsratsmitglied der DE-CIX Management GmbH, eines der größten deutschen Serviceprovider, hat der Beschwerdeführer zu 6 Zugriff auf große Mengen hochsensibler Daten, einschließlich der Abhörziele des Bundesministeriums des Inneren (BMI) und des Bundesnachrichtendienstes (BND). Diese Informationen über drohende Gefahren für die freiheitliche demokratische Grundordnung oder den Bestand oder die Sicherheit des Bundes oder eines Landes, die sich aus den Anordnungen vom BMI und BND ableiten lassen, werden als Verschlusssache eingestuft. An diesen Daten dürften ausländische Geheimdienste und kriminelle Hacker ein exorbitant großes Interesse aufweisen.

Ebenso macht ihn seine Tätigkeit als Sicherheitsberater für zahlreiche Internetdienstanbietern zum attraktiven Angriffsziel für kriminelle Hacker oder ausländische Nachrichtendienste. Ein Angriff auf das IT-System des Beschwerdeführers zu 6 verschafft dem Angreifer Zugriff auf die Internetdienstleistungen seiner Kunden, einschließlich aller Bestands- und Verkehrsdaten dessen Kundenkreises. Dies kann unter Umständen die Daten mehrerer tausend Kunden betreffen, zudem könnte sich der Angreifer Zugriff auf einzelne Leitungen verschaffen und diese manipulieren.

In Bezug auf einen Kunden des Beschwerdeführers zu 6 betrifft dies auch die gesamte Interne-tinfrastruktur eines Landkreises, einschließlich der Verwaltungsstrukturen. Der Zugriff auf diese Daten ermöglicht tiefgreifende Einblicke in die Verwaltungsabläufe des Landkreises, seiner sicherheitsrelevanten Belange sowie Informationen über die ansässigen Bürger, deren Daten beim Einwohnermeldeamt hinterlegt sind.

Schließlich ist der Beschwerdeführer auch durch seine Mitgliedschaft im Vorstand des ECO, dem Verband der Internetwirtschaft, einem hohen Risiko eines Hackerangriffs ausgesetzt, der wiederum weitreichende Folgen hätte. Innerhalb des Verbandes werden beispielsweise vertrauliche Informationen zu aktuellen Sicherheitslücken oder laufenden politischen Beratungen ausgetauscht.

Da der Beschwerdeführer zu 6 aus beruflichen Gründen häufig auf Reisen ist, laufen sämtliche Kommunikationen auf seinem Notebook zusammen. Die Sicherheit seines IT-Systems zu gewährleisten, ist damit in allen Funktionen des Beschwerdeführers eine grundrechtlich geschützte Kerntätigkeit. Doch auch wenn der Beschwerdeführer zu 6 alle nach dem Stand der Technik möglichen Sicherheitsvorkehrungen trifft, besteht dennoch eine Gefahr für die Vertraulichkeit der geschützten Informationen, da in diesen Systemen immer wieder unvermeidbare Sicherheitslücken auftreten können, die vom Land Hessen geduldet bzw. sogar gefördert werden.

Auch die Beschwerdeführerin zu 7 ist damit beauftragt, IT-Sicherheitsdienstleistungen zu erbringen und die IT-Systeme seiner Kund*innen sicher zu halten. Sie trägt die Verantwortung für die Vertraulichkeit der Daten ihrer Kund*innen. Ein Trojaner, welcher in ihr IT-System eindringt, kann zum einen Daten über ihr Geschäftsmodell, Arbeitsweise und Strategien auslesen und damit weitreichende Einblicke in ihre Tätigkeit gewinnen. Zum anderen kann ein Angriff auf ihr IT-System auch einen erleichterten Zugriff auf die IT-Systeme ihrer Kund*innen ermöglichen. Die Sicherheit ihres IT-Systems sowie des IT-Systems ihrer Kund*innen zu gewährleisten ist damit eine grundrechtlich geschützte Kerntätigkeit der Beschwerdeführerin zu 7.

e) Eigene, gegenwärtige und unmittelbare Betroffenheit

Die Beschwerdeführer*innen sind auch selbst, gegenwärtig und unmittelbar von den angegriffenen Regelungen betroffen, § 90 Abs. 1 BVerfGG. §§ 15b, 15c HSOG betrifft die Beschwerdeführer*innen zu 1 bis 7 unmittelbar in ihren Grundrechten aus Art. 2 Abs. 1 i.V. mit Art. 1 Abs. 1 GG bzw. Art. 2 Abs. 1 GG, weil es zu ihrer Beschwer keines weiteren gegen sie gerichteten Akts bedarf. Vielmehr folgt ihre Betroffenheit gerade aus der durch staatliche Stellen erhöhten Gefahr für ihre IT-Systeme, die daraus resultiert, dass die Polizei Hessens wegen §§ 15b, 15c HSOG ihnen bekanntwerdende Sicherheitslücken unter Verletzung ihrer staatlichen Schutzpflicht gegenüber den Beschwerdeführer*innen nicht an die Hersteller der betroffenen Programme und IT-Systeme meldet.
Wäre für die Unmittelbarkeit der Grundrechtsverletzung demgegenüber daran anzuknüpfen, dass hessische Behörden eine bestimmte Schwachstelle geheim halten, um sie für Maßnahmen nach §§ 15b, 15c HSOG auszunutzen und genau diese durch Dritte für einen Hackerangriff auf ein IT-System der Beschwerdeführer*innen ausgenutzt würde, dann wäre der gerichtliche Rechtschutz unmöglich, da die Beschwerdeführer*innen von diesen Tatsachen, insbesondere den konkreten den Behörden bekannten Schwachstellen, keine Kenntnis erlangen würden,

> vergleiche hierzu im Fall des sogenannten „Großen Lauschangriffs", BVerfGE 109, 279 (306); 133, 277 (311 f.).

Die Beschwerdeführer*innen sind auch selbst und gegenwärtig von den Ermächtigungen in §§ 15b, 15c HSOG betroffen, weil sie IT-Systeme nutzen und auf ihre Integrität und Vertraulichkeit in besonderem Maße angewiesen sind. Hinsichtlich der Bedrohung durch Hackerangriffe speziell zu ihren Lasten sei auf die obigen Ausführungen zur besonderen Schutzbedürftigkeit und Sensibilität ihrer IT-Systeme hingewiesen.

IV. Subsidiarität der Verfassungsbeschwerde

Gegen formelle Gesetze ist ein Rechtsweg nicht gegeben, weshalb § 90 Abs. 2 Satz 1 BVerfGG der Verfassungsbeschwerde nicht entgegensteht. Aber auch die Subsidiarität der Verfassungsbeschwerde steht der Zulässigkeit nicht entgegen. Es ist den Beschwerdeführer*innen nicht möglich oder zumindest nicht zumutbar, gegen den Vollzug der angegriffenen Normen vorzugehen und sich so einen indirekten Rechtsschutz gegen diese Normen zu verschaffen.

Die Beschwerdeführer*innen erhalten von den angegriffenen Maßnahmen keine Kenntnis. Insoweit ist auf die Ausführungen zur unmittelbaren Beschwer zu verweisen.

Auch ein vorbeugender Rechtsschutz in Gestalt einer vorbeugenden Unterlassungs- oder Feststellungsklage ist den Beschwerdeführer*innen nicht eröffnet. Solche Klagen setzen nach gefestigter Rechtsprechung voraus, dass sich ein drohendes Verwaltungshandeln bzw. ein zukünftiges Rechtsverhältnis bereits hinreichend konkret abzeichnet und die für eine Rechtmäßigkeitsprüfung erforderliche Bestimmtheit aufweist,

> vgl. zur vorbeugenden Unterlassungsklage BVerwGE 45, 99 (105); BVerwG BeckRS 1981, 31248115; BVerwG, Urteil vom 13. Dezember 2017 – 6 A 6.16 –, juris, Rn. 12; Pietzcker, in: Schoch/Schneider/Bier, VwGO, § 42 Abs. 1 Rn. 163; zur Feststellungsklage BVerwGE 59, 310

(318); BVerwG NVwZ 1988, 430 (431); BVerwG NVwZ 2017, 791; BVerwG NVwZ 2018, 1476 (1482); Pietzcker, in: Schoch/Schneider/Bier, VwGO, § 43 Rn. 21.

Eine konkrete Bestimmung drohender Überwachungsmaßnahmen und anschließender Datenübermittlungen oder Datenanalysen ist den Beschwerdeführerinnen jedoch nicht möglich. Hierzu müssten die Beschwerdeführerinnen ein konkretes behördliches Verfahren bezeichnen können, in dessen Rahmen ihnen eine Überwachung – sei es als Kontaktpersonen oder als Drittbetroffenen – droht. Aus ihrer Betroffenenperspektive lassen sich solche Verfahren im Voraus aber nicht absehen.

Kenntnis von einem laufenden Verfahren können die Betroffenen frühestens erlangen, wenn die hessische Polizei offene Gefahrenabwehrmaßnahmen durchführt oder das Verfahren in ein offenes strafrechtliches Ermittlungsverfahren überleitet. Dies wird allerdings zum einen keineswegs in jedem Fall geschehen. Zum anderen werden zu diesem Zeitpunkt die verdeckten Überwachungsmaßnahmen bereits abgeschlossen sein, so dass ein vorbeugender Rechtsschutz zu spät käme.
Als Alternative bliebe den Beschwerdeführerinnen lediglich eine vorbeugende Klage gegen unbestimmte Überwachungsmaßnahmen in unbestimmten Verfahren. Eine solche Klage „ins Blaue hinein" sprengte jedoch den in langjähriger Rechtsprechung entwickelten Rahmen des vorbeugenden Rechtsschutzes und wäre aller Voraussicht nach unzulässig. Selbst wenn dies anders zu sehen wäre, wäre ein solcher Rechtsschutz so inadäquat, dass der Subsidiaritätsgrundsatz nicht dazu zwänge, ihn vorrangig zu ergreifen. Soweit nämlich die Beurteilung einer Norm allein spezifisch verfassungsrechtliche Fragen aufwirft, die das Bundesverfassungsgericht zu beantworten hat, ohne dass von einer vorausgegangenen fachgerichtlichen Prüfung verbesserte Entscheidungsgrundlagen zu erwarten wären, bedarf es einer vorangehenden fachgerichtlichen Entscheidung nicht,

BVerfG, Beschluss vom 18. Dezember 2018 – 1 BvR 2795/09, 1 BvR 3187/10 –, Rn. 44, NJW 2019, 842 (843).

So läge der Fall bei einer vorbeugenden Unterlassungs- oder Feststellungsklage gegen verdeckte Überwachungsmaßnahmen nach den angegriffenen Regelungen. Da die Beschwerdeführer*innen konkrete Überwachungsanlässe im Voraus nicht absehen und nicht benennen können, müsste eine solche Klage darauf gerichtet sein, eine Überwachung der Beschwerdeführerinnen nach den angegriffenen Regelungen *generell* zu unterlassen. Diese Klage wäre nur begründet, wenn es *keinen* denkbaren Sachverhalt gäbe, in dessen Rahmen die Beschwerdeführerinnen einer solchen Überwachung ausgesetzt werden dürfen. Dies ließe sich nur annehmen, wenn die angegriffenen Regelungen auch bei restriktiver Interpretation und unabhängig von ihrer tatsächlichen Handhabung verfassungswidrig wären. Ausführungen zur Auslegung und Anwendung der Normen könnten die Fachgerichte daher allenfalls als obiter dicta machen, zu denen sie nicht gehalten sind und deren bloße Möglichkeit unter Subsidiaritätsgesichtspunkten keinen fachgerichtlichen Rechtsschutz gebieten kann. Vielmehr wäre eine Aufklärung der einfachrechtlichen Rechtslage und der tatsächlichen Gegebenheiten im Verwaltungsprozess nicht angezeigt. Das verwaltungsgerichtliche Verfahren wäre vielmehr materiell als reiner Verfassungsprozess zu führen, was der Subsidiaritätsgrundsatz gerade nicht verlangt,

„Soweit die Beurteilung einer Norm allein spezifisch verfassungsrechtliche Fragen aufwirft, die das Bundesverfassungsgericht zu beantworten hat, ohne dass von einer vorausgegangenen fachgerichtlichen Prüfung verbesserte Entscheidungsgrundlagen zu erwarten wären, bedarf es einer vorangehenden fachgerichtlichen Entscheidung nicht“ vgl. Beschluss des Ersten Senats vom 18. Dezember 2018, 1 BvR 2795/09, Rn. 44; BVerfGE 123, 148 (172 f.); 138, 261 (271 f.); 143, 246 (322); stRspr.

Die Beschwerdeführer*innen können unter dem Gesichtspunkt der Subsidiarität der Verfassungsbeschwerde auch nicht darauf verwiesen werden, ihren Auskunftsanspruch aus § 26 HVSG gegen das Landesamt geltend zu machen und in dem verwaltungsgerichtlichen Verfahren ihre verfassungsrechtlichen Argumente gegen die angegriffenen Ausschlusstatbestände vorzubringen. Ein solches Vorgehen ist den Beschwerdeführer*innen nicht zumutbar, weil ein wirksamer fachgerichtlicher Rechtsschutz gegen eine Auskunftsverweigerung im Einzelfall nicht durchweg gewährleistet ist.

Grund hierfür ist, dass das Landesamt gemäß § 26 Abs. 3 HVSG
nicht verpflichtet ist, eine Auskunftsverweigerung zu begründen. Fehlt eine Begründung, so kann der Auskunftspetent vor Gericht nicht umfassend darlegen, weshalb die vom Landesamt für die Auskunftsverweigerung herangezogenen Gründe unzureichend sind. Auch Bedenken gegen einen der gesetzlichen Ausschlusstatbestände kann der Petent dann allenfalls pauschal ins Blaue hinein und nicht in Bezug auf den konkreten Einzelfall und den in diesem Fall maßgeblichen Ausschlusstatbestand vorbringen. Die Gründe für die Auskunftsverweigerung können gerichtlich (zunächst) nur in einem In-Camera-Verfahren gemäß § 99 Abs. 2 VwGO überprüft werden. Vom Prozessstoff dieses Verfahrens erhält der Auskunftspetent jedoch wiederum keine umfassende Kenntnis, so dass er sich auch in diesem Rahmen nicht detailliert zu der Auskunftsverweigerung und den für sie herangezogenen Gründen äußern kann. So ist es im Verwaltungsgerichtsverfahren der Beschwerdeführerin zu 1 vor dem Verwaltungsgericht Kassel geschehen. Die Beschwerdeführer*in erhielt selbst keine umfassende Erläuterung zu den Auskunftsverweigerungen, ebenso wenig wie das VG Kassel selbst.

Dementsprechend hat das angerufene Gericht in seinem Urteil zur Antiterrordatei auf eine Rechtssatzverfassungsbeschwerde gegen die diese Datei errichtenden Normen auch die Auskunftsregelung in § 10 Abs. 2 ATDG-a.F. überprüft,

vgl. BVerfGE 133, 277 (367 ff.).

Dabei versprach eine fachgerichtliche Überprüfung der Auskunftsverweigerung auf der Grundlage von § 10 Abs. 2 ATDG-a.F. noch eher einen wirksamen Rechtsschutz, als er in den Fällen des § 26 HVSG gegeben ist. Denn § 10 Abs. 2 ATDG-a.F. verwies auch auf § 19 Abs. 5 BDSG, der zumindest grundsätzlich vorsieht, dass die Auskunftsverweigerung zu begründen ist.

D. Begründetheit

Die Verfassungsbeschwerde ist begründet.

I. Grundrechtswidrigkeit der angegriffenen Regelungen im HVSG

Die angegriffenen Überwachungsermächtigungen im HVSG sind zu weit und zudem teilweise zu unbestimmt gefasst (unter 1).
Die transparenzschaffenden Vorgaben zu Benachrichtigungspflichten und Auskunftsrechten Betroffener verfehlen die verfassungsrechtlichen Anforderungen (unter 2).
Die Ermächtigungen des Landesamts für Verfassungsschutz zu Datenverarbeitung und Übermittlungen an andere öffentliche und nicht-öffentliche Stellen stehen nicht mit den verfassungsrechtlichen Anforderungen im Einklang (unter 3).

1. Grundrechtswidrigkeit der angegriffenen Überwachungsermächtigungen

Auf der Grundlage der in der Rechtsprechung des angerufenen Gerichts entwickelten grundrechtlichen Maßstäbe für präventiv ausgerichtete Eingriffstatbestände im Sicherheitsrecht (unter a) weisen die Ermächtigungen im HVSG zur Ortung von Mobilfunkendgeräten in § 9 Abs. 1 HVSG, zu besonderen Auskunftsersuchen bei Betreibern von Computerreservierungssystemen und Globalen Distributionssystemen für Flüge in § 10 Abs. 2 HVSG, zum Einsatz Verdeckter Mitarbeiterinnen und Verdeckter Mitarbeiter in § 12 Abs.1 HVSG und zum Einsatz von Vertrauensleuten in § 13 HVSG materielle Mängel auf (unter b-d).

a) Verfassungsrechtliche Maßstäbe

Die verfassungsrechtlichen Maßstäbe, denen die Tatbestände von Überwachungsermächtigungen im Verfassungsschutzrecht genügen müssen, lassen sich aus der Rechtsprechung des angerufenen Gerichts zum Sicherheitsrecht ableiten. Ausgangspunkt ist der Verhältnismäßigkeitsgrundsatz und insbesondere das Gebot der Verhältnismäßigkeit im engeren Sinne. Danach sind an die gesetzlichen Eingriffsschwellen desto höhere Anforderungen zu stellen, je schwerer der geregelte Überwachungseingriff wiegt. Dies kann dazu führen, dass eine bestimmte Überwachungsmaßnahme nicht zur Durchsetzung bestimmter Allgemeininteressen angewandt werden darf, weil die davon ausgehenden Grundrechtsbeeinträchtigungen schwerer wiegen als die durchzusetzenden Belange,

> vgl. BVerfGE 120, 274 (322).

Im Einzelnen knüpfen die verfassungsrechtlichen Anforderungen an die gesetzliche Eingriffsschwelle an zwei Parameter an: Erstens muss das Gesetz einen hinreichend gewichtigen Anlass für die jeweilige Überwachungsmaßnahme in normenklarer Weise regeln. Zweitens muss das Gesetz gewährleisten, dass die Zielperson der Überwachungsmaßnahme in einem hinreichenden Näheverhältnis zu dem Anlass der Maßnahme steht. Für die Konkretisierung der verfassungsrechtlichen Maßstäbe ist insbesondere bedeutsam, ob und inwieweit auf die Rechtsprechung des angerufenen Gerichts zu präventivpolizeilichen Überwachungsmaßnahmen zurückgegriffen werden kann, um Ermächtigungen im Verfassungsschutzrecht zu beurteilen.

Im Ausgangspunkt hat das angerufene Gericht wiederholt anerkannt, dass die unterschiedlichen Aufgaben und Befugnisse von Polizeibehörden und Nachrichtendiensten es grundsätzlich rechtfertigen, an Überwachungsermächtigungen im Nachrichtendienstrecht weniger strenge Anforderungen zu stellen als an entsprechende Ermächtigungen im Polizeirecht,

> vgl. BVerfGE 100, 313 (383); 120, 274 (330); 130, 151 (206); 133, 277 (325 ff.); kritisch mit der Forderung nach einer partiellen „Deprivilegierung der Geheimdienste" Wegener, VVDStRL 75 (2016), S. 293 (312 ff.).

Allerdings ist zugleich seit geraumer Zeit in der Rechtsprechung anerkannt, dass sich die verfassungsrechtlichen Anforderungen an die gesetzlichen Eingriffsschwellen auch im Nachrichtendienstrecht mit zunehmender Eingriffsintensität der jeweiligen Überwachungsmaßnahme verschärfen,

> vgl. beispielhaft zu Eingriffen in das Fernmeldegeheimnis BVerfGE 120, 274 (342 f.).

Bereits mehrfach hat zudem das angerufene Gericht deutlich gemacht, dass die Anforderungen an Überwachungsermächtigungen des Nachrichtendienstrechts bei besonders eingriffsintensiven Maßnahmen mit den Anforderungen an polizeirechtliche Ermächtigungen konvergieren. Für solche Maßnahmen hat das angerufene Gericht ausdrücklich ausgeführt, dass die verfassungsrechtliche Mindesteingriffsschwelle auch nicht deshalb abzusenken ist, weil die Nachrichtendienste aufgrund ihres spezifischen Auftrags zur Vorfeldaufklärung nicht dazu berufen sind, konkrete Gefahren mit imperativen Mitteln abzuwehren,

> vgl. zur Online-Durchsuchung BVerfGE 120, 274 (329 ff.); zum Abruf bevorrateter Telekommunikations-Verkehrsdaten BVerfGE 125, 260 (331 f.). Für die Wohnraumüberwachung ergibt sich diese Konvergenz bereits aus Art. 13 Abs. 4 GG, der alle präventiv ausgerichteten Überwachungen an denselben Maßstab bindet und nicht zwischen unterschiedlichen Behörden differenziert.

Im Gegenteil hat das angerufene Gericht die Aktivitäten der Nachrichtendienste als besonders belastend bewertet, weil die gesamte Tätigkeit geheim erfolgt und „das Gefühl des unkontrollierbaren Beobachtetwerdens" befördert,

> BVerfGE 125, 260 (332).

Auf der Grundlage des Urteils zum BKA-Gesetz, das die verfassungsrechtlichen Anforderungen an präventivpolizeiliche Überwachungsermächtigungen präzisiert und konsolidiert hat, lassen sich die Maßstäbe auch für Ermächtigungen im Nachrichtendienstrecht weiter schärfen. In diesem Urteil hat das angerufene Gericht eingriffsintensive Überwachungsmaßnahmen an das Erfordernis einer konkreten Gefahr als einheitliche Mindesteingriffsschwelle gebunden. Zugleich hat das Gericht den verfassungsrechtlichen Begriff der konkreten Gefahr von dem polizeirechtlichen Gefahrbegriff entkoppelt und im Verhältnis zu diesem erweitert.
Eine konkrete Gefahr im verfassungsrechtlichen Sinne liegt danach nicht nur dann vor, wenn situationsbezogen ein Schaden mit hinreichender Wahrscheinlichkeit droht, wie es der polizeirechtliche Gefahrbegriff verlangt. Daneben könne eine „hinreichend konkretisierte Gefahr" auch schon bestehen, „wenn sich der zum Schaden führende Kausalverlauf noch nicht mit hinreichender Wahrscheinlichkeit vorhersehen lässt, sofern bereits bestimmte Tatsachen auf eine im Einzelfall drohende Gefahr für ein überragend wichtiges Rechtsgut hinweisen." Diese Tatsachen müssten „zum einen den Schluss auf ein wenigstens seiner Art nach konkretisiertes

und zeitlich absehbares Geschehen zulassen, zum anderen darauf, dass bestimmte Personen beteiligt sein werden, über deren Identität zumindest so viel bekannt ist, dass die Überwachungsmaßnahme gezielt gegen sie eingesetzt und weitgehend auf sie beschränkt werden kann." (Zumindest) in Bezug auf terroristische Straftaten hat das angerufene Gericht es darüber hinaus für ausreichend gehalten, „wenn zwar noch nicht ein seiner Art nach konkretisiertes und zeitlich absehbares Geschehen erkennbar ist, jedoch das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass sie solche Straftaten in überschaubarer Zukunft begehen wird",

> BVerfGE 141, 220 (272).

Insbesondere die zweite Formulierung zielt erkennbar auf eine Ergänzung der situationsbezogenen Schadensprognose des hergebrachten polizeirechtlichen Gefahrbegriffs um eine personenbezogene Gefährlichkeitsprognose, die allerdings auf hinreichend aussagekräftigen Tatsachen beruhen muss,

> vgl. für einen Ansatz zur rechtsdogmatischen Erfassung und Rationalisierung personenbezogener Prognoseurteile Bäcker, Kriminalpräventionsrecht, 2015, S. 205 ff.

Ob diese Erweiterung des verfassungsrechtlichen Gefahrbegriffs durchweg eine tragfähige Grundlage für eine rechtsstaatskonforme Konsolidierung des Polizeirechts darstellt, oder ob es sich – so der Eindruck des Unterzeichners – um eine konzeptionell problematische Verwischung unterschiedlicher Tatbestandskategorien und hinsichtlich von höchst eingriffsintensiven Überwachungsmaßnahmen wie Wohnraumüberwachung und „Online-Durchsuchung" um eine bedenkliche Aufweichung rechtsstaatlicher Grundsätze handelt, mag hier offenbleiben. Jedenfalls ist der erweiterte verfassungsrechtliche Gefahrbegriff auch für das Nachrichtendienstrecht anschlussfähig:
Einerseits ermöglicht der erweiterte verfassungsrechtliche Gefahrbegriff Überwachungsmaßnahmen bereits im Vorfeld akuter Krisenlagen, das in besonderem Maße die Domäne der nachrichtendienstlichen Aufklärung darstellt. Insbesondere ein personenbezogener Prognosetatbestand kommt dem spezifischen Aufklärungsauftrag des Verfassungsschutzes entgegen, indem er Überwachungsmaßnahmen gegen „Gefährder" bereits im Vorfeld klar konturierter schadensträchtiger Situationen ermöglicht.
Andererseits schirmt der erweiterte verfassungsrechtliche Gefahrbegriff das Risiko ab, dass gerade die Nachrichtendienste Überwachungsmaßnahmen von hoher Eingriffsintensität im Wesentlichen auf allgemeine Erfahrungssätze stützen könnten, deren Gebrauch rechtlich nicht näher angeleitet wird und die möglicherweise nur sehr grobe Prognosen zulassen. Denn der erweiterte verfassungsrechtliche Gefahrbegriff ermöglicht Überwachungsmaßnahmen gerade nur gegenüber Personen, die aufgrund ihres Vorverhaltens belastbar als „gefährlich" gekennzeichnet werden können.
Die von dem angerufenen Gericht umrissene personenbezogene Gefährlichkeitsprognose eignet sich daher besonders dazu, personengerichtete Überwachungsmaßnahmen der Nachrichtendienste im benötigten Umfang zu ermöglichen und sie zugleich hinreichend trennscharf zu begrenzen.
Damit ist nach der partiellen Neukonzeption der verfassungsrechtlichen Anforderungen an das Polizeirecht im Urteil zum BKA-Gesetz nunmehr auch eine Anpassung der verfassungsrechtlichen Anforderungen an das Nachrichtendienstrecht angezeigt.
Personengerichtete Überwachungsmaßnahmen hoher Eingriffsintensität sind auch im Nachrichtendienstrecht an eine situationsbezogene Schadens- oder eine personenbezogene

Gefährlichkeitsprognose zu binden, wie sie das angerufene Gericht für das Polizeirecht entwickelt hat. Eine Absenkung der verfassungsrechtlichen Mindesteingriffsschwelle ist für solche Überwachungsmaßnahmen nach der Erweiterung des verfassungsrechtlichen Gefahrbegriffs nicht (mehr) angezeigt,

> vgl. andeutungsweise bereits BVerfGE 141, 220 (340): danach bedürfen „ungeachtet ihres im Wesentlichen auf das Vorfeld von Gefahren beschränkten Handlungsauftrags“ auch Datenerhebungen von Verfassungsschutzbehörden grundsätzlich einer „konkretisierten Gefahrenlage“.

Zur Einstufung der Eingriffsintensität der Aufklärungsmaßnahmen kommt es bei personengerichteten Maßnahmen ohne besondere Streubreite vor allem darauf an, ob sie in besondere Rückzugsbereiche der Privatheit eindringen, auf einem Bruch schutzwürdigen personengebundenen Vertrauens beruhen, Wahrnehmungsschranken insbesondere durch technische Mittel oder ein planvoll verdecktes Vorgehen überwinden oder Eigenschaften, Verhalten oder Sozialkontakte der betroffenen Person in besonderem Maße für die Überwachungsbehörde verfügbar machen.

b) Ortung von Mobilfunkendgeräten, § 9 Abs.1 HVSG

Mit § 9 Abs. 1 HVSG ist eine eigene Ermächtigungsgrundlage für die Ortung von Mobilfunkendgeräten geschaffen worden. Abweichend vom früheren § 5 Abs. 2 HVSG setzt der Einsatz das Vorliegen von tatsächlichen Anhaltspunkten für eine schwerwiegende Gefahr für die von § 2 HVSG umfassten Schutzgüter voraus.
Die Eingriffsermächtigung verletzt die Beschwerdeführer*innen in ihrem Grundrecht auf informationelle Selbstbestimmung, denn sie ist gemessen an der Eingriffsintensität unverhältnismäßig weit gefasst. Die von dieser Regelung ermöglichte Ortungsmaßnahme kann eine hohe Eingriffsintensität erreichen. Dies ist insbesondere anzunehmen, wenn die Maßnahme über einen längeren Zeitraum hinweg andauert. In einem solchen Fall ermöglicht sie die Erstellung eines umfassenden Bewegungsprofils des Betroffenen, mit dessen Hilfe auch das zukünftige Bewegungsverhalten prognostiziert werden kann. Zudem können die Ortungsdaten mit weiteren – auch öffentlich zugänglichen – Daten verknüpft werden, um weitreichende Aussagen über die Lebensgestaltung des Betroffenen zu ermöglichen,

> vgl. zur Eingriffsintensität der funktional vergleichbaren Observation mittels GPS BVerfGE 112, 304 (316 f.); BVerfGE 141, 220 (268). Ein instruktives Auswertungsbeispiel für die Verknüpfung von Mobilfunk-Standortdaten mit weiteren, teils öffentlich zugänglichen Kommunikationsdaten findet sich unter http://www.zeit.de/datenschutz/malte-spitz-vorratsdaten, zuletzt abgerufen am 01.07.2019.

Der potenziell hohen Eingriffsintensität der geregelten Maßnahme muss der Gesetzgeber durch eine hinreichend restriktive Eingriffsschwelle Rechnung tragen. § 9 Abs. 1 HVSG leistet dies nicht. Grund hierfür ist in erster Linie, dass die Regelung zu unbestimmt ist. Auf den ersten Blick scheint zwar das Erfordernis einer „schwerwiegenden Gefahr“ für die von § 2 HVSG umfassten Schutzgüter klar gefasst zu sein. Insbesondere scheint zur Konkretisierung dieses Erfordernisses ein Rekurs auf den polizeirechtlichen Gefahrbegriff nahezuliegen, der auch gewichtige Eingriffsmaßnahmen rechtfertigen kann. Jedoch zeigt sich bei näherer Betrachtung, dass der polizeirechtliche Gefahrbegriff hier nicht weiterführt. Stattdessen müsste

ein spezifisch nachrichtendienstlicher Gefahrbegriff gebildet werden, den das Gesetz jedoch nicht ansatzweise konkretisiert und dessen Konturen äußerst unscharf bleiben.
Der polizeirechtliche Gefahrbegriff kann zur Konkretisierung von § 9 Abs. 1 HVSG nicht herangezogen werden, weil er in engem Zusammenhang mit den polizeilichen Schutzgütern der öffentlichen Sicherheit und Ordnung steht und durch sie seine Konturen gewinnt. § 9 Abs. 1 HVSG nimmt diese Schutzgüter – aufgrund der unterschiedlichen Aufgaben von Polizei und Verfassungsschutz konsequent – nicht in Bezug. Die Norm nennt jedoch auch ansonsten keine Schutzgüter, die sinnvoller Gegenstand einer Schadensprognose im Sinne des polizeirechtlichen Gefahrbegriffs sein könnten. § 2 HVSG definiert keine Schutzgüter, sondern formuliert Aufklärungsauftrage des Landesamts für Verfassungsschutz. Allenfalls partiell und mittelbar lassen sich aus dieser Norm Güter ableiten, welche das Landesamt schützen soll. So mag man § 2 HVSG als Schutzgüter die freiheitlich demokratische Grundordnung, den Bestand oder die Sicherheit des Bundes oder eines Landes und die Amtsführung der Verfassungsorgane von Bund und Ländern entnehmen können. Allerdings sind die so gewonnenen Schutzgüter des Verfassungsschutzes fast durchweg sehr unscharf gefasst. Je nachdem, wie sie verstanden werden, lässt sich eine polizeirechtliche Gefahr für eines dieser Schutzgüter so gut wie nie oder fast immer annehmen. Dem kann auch der Verweis des § 3 Abs. 1 HVSG auf die Begriffsbestimmungen des § 4 BVerfSchG nicht abhelfen. Zum einen erschwert schon die Normenkette von § 9 HVSG über §§ 2, 3 HVSG zu § 4 BVerfSchG das Normenverständnis und die Bestimmung der Bezugspunkte der Eingriffsschwelle. Zum anderen sind die Gefährdungstatbestände des § 4 BVerfSchG so eng definiert, dass die Bezugnahme zur Bestimmung der Eingriffsschwelle des § 9 HVSG nicht weiterhilft. So müssten Bestrebungen gegen den Bestand des Bundes oder eines Landes eine Fremdherrschaft anstreben, Bestrebungen gegen die Sicherheit des Bundes oder eines Landes auf eine erhebliche Beeinträchtigung ihrer Funktionsfähigkeit gerichtet sein und Bestrebungen gegen die freiheitlich-demokratische Grundordnung darauf gerichtet sein, elementare Verfassungsgrundsätze zu beseitigen. So definiert, können selbst hochgradig gewalttätige Gruppierungen die freiheitlich demokratische Grundordnung als konstitutives Element der tatsächlichen Verfassungsordnung der Bundesrepublik und des Landes Hessen ebenso wenig ernsthaft bedrohen wie den Bestand oder die generelle Sicherheit des Bundes oder eines Landes.

Angesichts dieser Interpretationsprobleme liegt nahe, den Gefahrbegriff im Verfassungsschutzrecht eigenständig zu verstehen und vom polizeirechtlichen Gefahrbegriff abzukoppeln. So geht, soweit ersichtlich, auch die Praxis vor. Allerdings weist der spezifisch nachrichtendienstliche Gefahrbegriff praktisch keine Konturen auf und geht letztlich kaum über das Erfordernis tatsächlicher Anhaltspunkte hinaus, das gemäß Art. 5 Abs. 1 Nr. 1 HVSG für alle Überwachungsmaßnahmen des Verfassungsschutzes zu beachten ist,

> vgl. beispielhaft den Konkretisierungsversuch bei VG Berlin, Urteil vom 7. September 2016 – 1 K 12.15 –, juris, Rn. 26 ff.

Das weitere Merkmal einer „schwerwiegenden“ Gefahr, das gemeinhin auf das Schädigungspotenzial der betreffenden Bestrebung bezogen wird, kann diese Unschärfe nicht beseitigen, da die relevanten Schutzgüter unklar bleiben. Nur mit Blick auf bestimmte Schutzgüter lässt sich das Schädigungspotenzial aber überhaupt bestimmen.
Schließlich führt die Unschärfe des nachrichtendienstlichen Gefahrbegriffs dazu, dass auch die zugehörigen Betroffenenregelungen in § 9 Abs. 2 i.V. mit § 3 Abs. 2 G 10 unklar werden. Wenn sich nicht klar angeben lässt, wann eine nachrichtendienstliche Gefahr besteht, kann auch nicht bestimmt werden, wer für diese Gefahr verantwortlich ist oder sonst zu ihr beige-

tragen hat. Ein sehr weites Verständnis der Gefahrenquelle geht wiederum aus der Gesetzesbegründung zu § 4 HVSG hervor, wonach jedenfalls die „Beobachtung durch das Landesamt nicht von individuellen und subjektiven Beiträgen der betroffenen Person oder deren intentionalen Beteiligung an Handlungen zur Beseitigung der freiheitlichen demokratischen Grundordnung“ abhänge, wesentlich sei die Mitgliedschaft in dem Personenzusammenschluss,

LT-Drucksache 19/5412, Seite 30.

Übertragen auf die Eingriffsschwelle des § 9 Abs. 1 HVSG reicht es folglich möglicherweise aus, wenn von dem Personenzusammenschluss eine schwerwiegende Gefahr für die nicht näher bestimmbaren Schutzgüter ausgeht, um die Mobilfunkendgeräte einzelner Mitglieder zu orten. Begrifflich ist der Verweis auf § 3 Abs. 2 Artikel-10-Gesetz zudem unpassend, da er auf die Verdächtigeneigenschaft einer Person abstellt. In § 9 HVSG geht es um die Mobilfunkortung zur Abwehr einer schwerwiegenden Gefahr und nicht um die Verfolgung von Straftaten.

Dem Befund, dass der nachrichtendienstliche Gefahrbegriff des § 9 Abs. 1 HVSG zu unbestimmt ist, kann nicht das Urteil des angerufenen Gerichts zum nordrhein-westfälischen Verfassungsschutzgesetz entgegengehalten werden. In diesem Urteil hat das Gericht zwar einen gleichartigen Eingriffstatbestand für eine vergleichbar eingriffsintensive Überwachungsmaßnahme verfassungsrechtlich gebilligt,

vgl. zum Abruf von Kontoinhalten BVerfGE 120, 274 (348 f.).

Im Lichte der jüngeren Rechtsprechung des angerufenen Gerichts bedarf es jedoch einer Neubewertung. Das angerufene Gericht hat sich mit den in Bezug genommenen Schutzgütern des Verfassungsschutzes in der damaligen Entscheidung nicht auseinandergesetzt und daher auch die Unschärfe des nachrichtendienstlichen Gefahrbegriffs nicht untersucht. Das angerufene Gericht hat jedoch in ebendieser Entscheidung darauf hingewiesen, dass auch Nachrichtendienste, deren Aufgabe in der Vorfeldaufklärung besteht, an den Verhältnismäßigkeitsgrundsatz gebunden sind. Da die Eingriffsintensität der Datenerhebung unabhängig von den weiteren Befugnissen der Behörde die Gleiche sei, bestehe kein Anlass zu behördenbezogenen Differenzierungen,

BVerfGE 120, 274 (329 f.).

Zum Gefahrenbegriff im Rahmen der Ermächtigung zur Online-Durchsuchung führt das angerufene Gericht aus, selbst „wenn es nicht gelingen sollte, speziell auf im Vorfeld tätige Behörden zugeschnittene gesetzliche Maßgaben für den Eingriffsanlass zu entwickeln, die dem Gewicht und der Intensität der Grundrechtsgefährdung in vergleichbarem Maße Rechnung tragen wie es der überkommene Gefahrenbegriff etwa im Polizeirecht leistet, wäre dies kein verfassungsrechtlich hinnehmbarer Anlass, die tatsächlichen Voraussetzungen für einen Eingriff […] abzumildern“,

BVerfGE 120, 274 (331 f.).

Anders als zum Zeitpunkt der zitierten Entscheidung steht mit der im neueren Urteil zum BKA-Gesetz vorgenommenen Ausdehnung des Gefahrbegriffs von einer rein situations- zu einer auch personenbezogenen Schadensprognose nunmehr ein solcher trennschärferer verfassungsrechtlicher Kontroll- und fachrechtlicher Regulierungsansatz zur Verfügung, der dem

Gewicht und der Intensität des Grundrechtseingriffs Rechnung trägt. Eines darüberhinausgehenden spezifisch nachrichtendienstlichen Gefahrbegriffs, dessen Gehalt sich nicht klar bestimmen lässt, bedarf es daneben nicht.

c) besondere Auskunftsersuchen, § 10 Abs. 2 Satz 1 Nr. 1 HVSG

§ 10 HVSG ersetzt die bisher in § 4a HVSG a.F. enthaltene Befugnis für besondere Auskunftsersuchen und erstreckt den Auskunftsanspruch in § 10 Abs. 2 Satz 1 Nr. 1 HVSG auf alle Verkehrsunternehmen, sowie die Betreiber von Computerreservierungssystemen und die Betreiber von globalen Distributionssystemen für Flüge.
Bei den von § 10 Abs. 2 Satz 1 Nr. 1 HVSG erfassten Auskünften handelt es sich um einen intensiven Eingriff in die grundrechtlich geschützte informationelle Selbstbestimmung gemäß Art. 2 Abs. 1 GG i.V. mit Art. 1 Abs. 1 GG. Demgegenüber sind die Eingriffsvoraussetzungen zu unbestimmt und genügen nicht den Verhältnismäßigkeitsanforderungen.
Die Erstreckung des Auskunftsanspruches auf sämtliche Verkehrsunternehmen ermöglicht Auskünfte bei der Bahn, den Fernbusunternehmen, bei Carsharinganbietern, bei Mitfahrgelegenheitsportalen und allen weiteren Transportdienstleistungen, die personenbezogene Daten erheben und speichern.

Während also bislang mit dem Luftverkehr ausschließlich ein geringer Teil der individuellen Mobilität abgedeckt war, ermöglicht die Erweiterung nunmehr unter Umständen eine nahezu lückenlose Kontrolle des individuellen Bewegungsverhaltens, jedenfalls soweit zur Fortbewegung Verkehrsdienstleister in Anspruch genommen werden. Die Inanspruchnahme und Kombination verschiedener Mobilitätsdienstleister anstelle des privaten Fahrzeugs nimmt aktuell zu. Ein Auskunftsanspruch des Landesamts gegenüber sämtlichen Transportunternehmen ermöglicht folglich in einigen Fällen die Erstellung umfassender Bewegungsprofile einer Person, insbesondere wenn Auskünfte verschiedener Transportunternehmen kombiniert werden. Der Auskunftsanspruch eröffnet damit weitreichende Einblicke in die Lebensgestaltung und bedarf einer ausreichend bestimmten und hinreichend restriktiven Eingriffsschwelle.

Diesen Anforderungen genügt § 10 Abs. 2 Satz 1 Nr. 1 HVSG nicht. Der dort normierte Auskunftsanspruch setzt lediglich tatsächliche Anhaltspunkte für Bestrebungen und Tätigkeiten nach § 2 Abs. 2 HVSG voraus. Diese allgemeine Eingriffsschwelle des § 5 Abs. 1 HVSG wird in § 10 Abs. 2 Satz 2 HVSG nur in Bezug auf Bestrebungen nach § 2 Abs. 2 Nr. 1 HVSG qualifiziert. Diese müssen eine besondere Gewaltaffinität aufweisen, um den Auskunftsanspruch zu begründen.
Wie weiter oben ausgeführt, sind die in § 2 Abs. 2 aufgeführten Bestrebungen und Tätigkeiten nahezu konturlos und beschreiben sehr unbestimmte Schutzgüter, die deutlich weiter als die polizeilichen Schutzgüter der öffentlichen Sicherheit und Ordnung gehen,

> vgl. dazu unter D I 1 b).

Der Unbestimmtheit dieser Eingriffsschwelle vermag auch die Qualifizierung der Bestrebungen nach § 2 Abs. 2 Nr. 1 HVSG nicht abzuhelfen. Schließlich sind auch andere Tätigkeiten und Bestrebungen nach § 2 Abs. 2 HVSG sehr weit gefasst und unbestimmt, beispielsweise die Bestrebungen nach § 2 Abs. 2 Nr. 4, die sich gegen den Gedanken der Völkerverständigung richten.

Vielmehr erfordert die Schwere des Eingriffs das Vorliegen einer konkreten Gefahr, wobei dabei nicht auf den konturlosen nachrichtendienstlichen Gefahrenbegriff unter Bezug auf die Schutzgüter des § 2 HVSG rekurriert werden sollte, sondern auf den im BKA-Gesetz-Urteil des angerufenen Gerichts entwickelten verfassungsrechtlichen Gefahrenbegriffs zurückgegriffen werden müsste,

> vgl. dazu unter D I 1 a).

d) Einsatz von verdeckten Mitarbeiter*innen und Vertrauensleuten, §§ 12, 13 HVSG

Der Einsatz von verdeckten Mitarbeitern und Vertrauensleuten wird in §§ 12, 13 HVSG erstmals eigenständig geregelt und ist nach § 5 Abs. 1 Nr. 1 HSVG zulässig, wenn tatsächliche Anhaltspunkte für Bestrebungen oder Tätigkeiten nach § 2 Abs. 2 HVSG bestehen. Das angerufene Gericht hat den Einsatz von Vertrauenspersonen und verdeckten Mitarbeitern im Urteil zum BKA-Gesetz zu Recht als einen sehr schwerwiegenden Grundrechtseingriff eingestuft, der allenfalls bei einer konkretisierten Gefahr im Sinne des Urteils zulässig sein kann (dazu (1)). Die angegriffenen Ermächtigungen erfüllen diese Voraussetzungen nicht und verletzen deshalb das allgemeine Persönlichkeitsgrundrecht und das Wohnungsgrundrecht (dazu (2))

(1) Einstufung als schwerwiegender Grundrechtseingriff

Das angerufene Gericht hat in seinem Urteil zum BKA-Gesetz ausdrücklich festgehalten, dass die Ausforschung durch Vertrauensleute und verdeckte Mitarbeiter*innen (die in § 20g Abs. 2 Nr. 4 und 5 BKAG a.F. als weiterer Unterfall der besonderen Mittel der Datenerhebung vorgesehen war) einen sehr schwerwiegendem Grundrechtseingriff bedeutet,

> BVerfGE 141, 220 (290) (wonach die in § 20g Abs. 2 BKAG a.F. geregelten Überwachungsmittel „auch sehr schwerwiegende Grundrechtseingriffe“ umfassen, „wie etwa […] das Ausnutzen von Vertrauen durch Verdeckte Ermittler oder Vertrauenspersonen“.) Aus dem Schrifttum s. gleichgerichtet etwa Dietrich, in: ders./Eiffler (Hrsg.), Handbuch des Rechts der Nachrichtendienste, 2017, VI, § 2 Rn. 94 (der deren Einsatz „zu den eingriffsintensivsten nachrichtendienstlichen Mitteln überhaupt“ zählt).

Gerade bei der längerfristigen Observation durch Verdeckte Mitarbeiter*innen und Vertrauenspersonen können unter Ausnutzung des Vertrauens des Betroffenen tiefgreifende Erkenntnisse über dessen persönliche Verhältnisse gewonnen werden, was wiederum zu einem besonders intensiven Grundrechtseingriff führt. Dies birgt die Gefahr, dass Verhaltensprofile über den Betroffenen erstellt werden können,

> BVerfGE 120, 274 (237).

Selbst in einer Frühphase der Ausforschung, in der eher ungezielt erste Erkenntnisse über eine Bestrebung beschafft werden sollen, können Verdeckte Ermittler und Vertrauenspersonen zur

Informationsgewinnung in erheblichem Ausmaß schutzwürdiges Vertrauen enttäuschen und so einen Grundrechtseingriff gehobener Intensität bewirken,

vgl. zum Vertrauensbruch als Kriterium für das Vorliegen eines Grundrechtseingriffs BVerfGE 120, 274 (345).

Konsequenterweise ist das Ausmaß des enttäuschten Vertrauens auch als Kriterium für die Bestimmung der Eingriffsintensität heranzuziehen,

in diese Richtung auch BVerfGE 141, 220 (269).

Ein derartiger Vertrauensbruch kann für die Betroffenen auch erhebliche psychische Folgen haben, die gleichfalls in die Bestimmung der Eingriffsintensität einzubeziehen sind. Zur Illustration sei auf die Berichte über die Einschleusung verdeckter Ermittler der Polizei in linke Kreise in Hamburg und Heidelberg verwiesen,

vgl. zu dem Hamburger Fall http://www.zeit.de/politik/2015-08/rote-flora-polizei-maria-block; zu dem Heidelberger Fall http://www.zeit.de/campus/2016/03/spitzel-uni-heidelberg-linke-szene (letzte Abrufe am 15. Mai 2019).

Zur Schwere des Eingriffs trägt auch die potenziell abschreckende Wirkung auf die Ausübung von Grundrechten durch Betroffene und ihr Umfeld bei. Wer befürchten muss, im Rahmen seines politischen Engagements, beispielsweise auf Veranstaltungen oder Demonstrationen, verdeckten Ermittlern und Vertrauensleuten zu begegnen, wird von Versammlungen und Meinungsäußerungen künftig eher Abstand nehmen.

Ein besonders schwerer Eingriff ist insbesondere dann anzunehmen, wenn Verdeckte Mitarbeiter*innen oder Vertrauenspersonen auf eine bestimmte Person angesetzt werden und nicht nur auf eine bestimmte Personengruppe, um deren Rolle und Vernetzung innerhalb der Bestrebung aufzuklären. Ein derartiger personengerichteter Einsatz kann sich auf einen erheblichen Teil der Lebensgestaltung der Betroffenen erstrecken und sensible Informationen zum Gegenstand haben. Auch insoweit mögen die Fälle aus Hamburg und Heidelberg als Illustration dienen.

Verdeckte Mitarbeiter*innen und Vertrauenspersonen haben im Verlaufe ihres Einsatzes häufig Gelegenheit und auch Veranlassung, die Wohnungen von Zielpersonen zu betreten. Dies kann zwecks Vornahme konkreter Ermittlungshandlungen geschehen oder sich schlicht aus dem sozialen Kontext ergeben. Im Gegensatz zu § 111c StPO ermächtigen §§ 12, 13 HVSG nicht ausdrücklich zum Betreten einer Wohnung. Sollte diese Befugnis gleichwohl von der Ermächtigungsnorm umfasst sein, liegt hierin ein schwerwiegender Eingriff in das Grundrecht auf Unverletzlichkeit der Wohnung aus Art. 13 Abs. 1 GG. Art 13 Abs. 1 GG gewährleistet den Bürger*innen, in ihrer Wohnung vom Staat in Ruhe gelassen zu werden. Die Wohnung stellt eine von staatlicher Kontrolle freie Sphäre individueller Lebensgestaltung dar,

BVerfGE 32, 54 (75) BVerfGE 89, 1 (12) BVerfGE 96, 44 (51).

Dringt der Staat mit verdeckt operierenden Beamten in die Wohnung ein, verletzt er diesen geschützten Raum. Dem steht auch nicht das Einverständnis des Wohnungsinhabers entgegen, denn dieser hat keine Kenntnis vom staatlichen Ermittlungsauftrag,

so auch Frister JZ 1997, 1130 (1132); Roxin StV 1998, 43ff.; Schneider NStZ 2004, 359 (366).

(2) Unzureichende Eingriffsschwelle

Angesichts der Schwere des Eingriffs genügen die Eingriffsschwellen in §§ 12 Abs. 1, 13 HVSG den verfassungsrechtlichen Anforderungen nicht und verletzen das allgemeine Persönlichkeitsrecht sowie das Wohnungsgrundrecht der Beschwerdeführer*innen zu 1-5.

Aus der Einstufung als schwerwiegenden Grundrechtseingriff hat das angerufene Gericht die grundrechtsdogmatische Konsequenz gezogen, dass für diese Eingriffe die verfahrensrechtliche Eingriffsschwelle des Richtervorbehalts greift, und es deshalb als nicht ausreichend angesehen, diesen nur für den Einsatz Verdeckter Mitarbeiter*innen vorzusehen, weil auch der Einsatz von Vertrauenspersonen „unter Umständen so tief in die Privatsphäre“ eingreife, dass seine Anordnung „einer unabhängigen Instanz, etwa einem Gericht, vorbehalten bleiben“ müsse,

vgl. BVerfGE 141, 220 (294).

Das angerufene Gericht hat zudem, wie generell für schwerwiegend in Grundrechte eingreifende Überwachungsmaßnahmen, auch für diese Maßnahmen die materielle Eingriffsschwelle der hinreichend konkretisierten Gefahr als unabdingbar angesehen, um die Verhältnismäßigkeit der Eingriffe zu gewährleisten,

vgl. BVerfGE 141, 220 (290 f.).

Es erachtete deshalb (auch insoweit, wie für die anderen besonderen Mittel der Datenerhebung) die Vorfeldbefugnis in § 20g Abs. 1 S. 1 Nr. 2 BKAG für zu unbestimmt und unverhältnismäßig. Danach sollte das Bundeskriminalamt personenbezogene Daten mit den besonderen Mitteln nach § 20g Abs. 2 BKAG auch erheben können über „die Person, bei der Tatsachen die Annahme rechtfertigen, dass sie“ terroristische Straftaten gemäß § 4a Abs. 1 Satz 2 BKAG „begehen wird“,

vgl. BVerfGE 141, 220 (228).

Das Bundesverfassungsgericht erklärte dies für zu weitgehend und sah den Einsatz von Vertrauensleuten und Verdeckten Ermittlern nur unter den erwähnten engeren Voraussetzungen einer konkretisierten Gefahr als verhältnismäßig an,

vgl. nochmals BVerfGE 141, 220 (290 f.).

Die sehr weit gefassten Ermächtigungsgrundlagen in §§ 12 Abs. 1, 13 HVSG erfüllen diese Voraussetzungen nicht. §§ 12 Abs. 1, 13 HVSG regeln selbst nicht die Voraussetzungen des Einsatzes Verdeckter Mitarbeiter*innen und Vertrauensleuten. Maßgeblich ist damit die allgemeine Vorgabe des § 5 Abs. 1 HVSG. § 5 Abs. 1 Nr. 1 HSVG selbst fordert nur, dass tatsächliche Anhaltspunkte für Bestrebungen oder Tätigkeiten nach § 2 Abs. 2 HVSG bestehen. Die Anknüpfung an die reine Aufgabenzuweisung aus §§ 5 Abs. 1, 2 Abs. 2 HVSG mag unbedenklich sein für den Einsatz nachrichtendienstlicher Mittel von geringer Eingriffsintensität,

mit denen der Verfassungsschutz in noch weitgehend diffusen Lagen Anhaltspunkte gewinnen soll, auf deren Grundlage gezieltere Maßnahmen eingesetzt werden soll. Gewichtigere Grundrechtseingriffe wie den Einsatz Verdeckter Ermittler oder Vertrauenspersonen kann er in Anbetracht der niedrigen Eingriffsschwelle hingegen nicht legitimieren. Insoweit ist auch für die Arbeit des Verfassungsschutzes auf den vom angerufenen Gericht entwickelten verfassungsrechtlichen Gefahrenbegriff zurückzugreifen,

> vgl. dazu oben unter D I 1 a).

Zumindest muss der Einsatz von Verdeckten Mitarbeitern und Vertrauensleuten an eine hinsichtlich des Ziels der Aufklärung qualifizierte Eingriffsschwelle gebunden werden.

Beispielhaft kann auf § 9a Abs. 1 Satz 2 BVerfSchG verwiesen werden, der einen solchen Einsatz auf die Aufklärung verfassungsfeindlicher Bestrebungen von erheblicher Bedeutung begrenzt, insbesondere wenn sie darauf gerichtet sind, Gewalt anzuwenden oder Gewaltanwendung vorzubereiten.

Der Bundesgesetzgeber hat einen Einsatz von Verdeckten Mitarbeiter*innen bzw. von Vertrauensleuten gegen nicht gewaltorientierte Bestrebungen gerade auch deshalb abgelehnt, weil er ihn als nicht angemessen ansah,

> Entwurf eines Gesetzes zur Verbesserung der Zusammenarbeit im Bereich des Verfassungsschutzes, BT-Drucks. 18/4654, Seite 26.

Die Abweichung vom BVerfSchG erklärt die hessische Gesetzesbegründung damit, dass das Landesamt einen erweiterten Beobachtungsauftrag hat, der nicht auf gewaltbereite Bestrebungen fokussiert ist,

> Gesetzesbegründung des Gesetzes zur Neuausrichtung des Verfassungsschutzes in Hessen, Hessischer Landtag, Drucks. 19/5412, Seite 40.

Allerdings ist auch das Bundesamt für Verfassungsschutz nicht nur für die Beobachtung gewaltbereiter Bestrebungen zuständig,

> vgl. § 3 Abs. 1 BVerfSchG. In der Gesetzesbegründung dazu (BT-Drucks. 18/4654, S. 26.) wird erläutert, dass der dauerhafte Einsatz verdeckter Ermittler auf besonders bedeutsame Bestrebungen beschränkt werden soll. Eine besondere Bedeutung sei generell bei einer Gewaltorientierung der Bewegung anzunehmen. Es sei aber nicht ausgeschlossen, dass es sich auch ohne eine Gewaltorientierung um eine Bestrebung von besonderer Bedeutung handele. Dafür sollen als Kriterien Größe, Einfluss und Abschottung der Bewegung herangezogen werden.

Abweichend von den entsprechenden Befugnissen in §§ 9, 9b BVerfSchG ist der Einsatz von Verdeckten Mitarbeitern und V-Leuten nach §§ 12, 13 HVSG auch für die Beobachtung von Bestrebungen und Tätigkeiten der organisierten Kriminalität gemäß § 2 Abs. 2 Nr. 5 HVSG zulässig. Diese Aufgabe sieht das BVerfSchG ebenso wenig wie der ganz überwiegende Teil der anderen Landesverfassungsschutzgesetze vor. Die Beobachtung der Organisierten Kriminalität ist kaum eingrenzbar, es entsteht dadurch die Gefahr einer Überschneidung mit der Gefahrenabwehr und Strafverfolgung,

wegen der Überschneidungsgefahr urteilte der Sächsische Verfassungsgerichtshof, dass sich der Verfassungs-schutz auf seine klassischen Aufgaben zu berufen habe, die sich mit denen des Bundesamts für Verfassungs-schutz decken würden, SächsVerfGH, NVwZ 2005, 13010, 1312; in Thüringen wurde eine entsprechende Zuständigkeit des Landesamts für Verfassungsschutz 2012 wieder abgeschafft, Begründung zum Thüringer Gesetz zur Änderung sicherheitsrelevanter Vorschriften, Seite 5; allgemeine Kritik an der Entfernung von den klassischen Aufgaben eines Nachrichtendienstes gab es auch von mehreren Stellen, so etwa zur Novelle des G 10 Wollweber, ZRP 2001, 213, 214; Huber, NJW 2001, 3296, 3297.

§§ 12, 13 HVSG verletzen darüber hinaus die vom angerufenen Gericht aufgestellten Verfahrensanforderungen, da sie keine richterliche Anordnung der Maßnahmen vorsehen,

BVerfGE 141, 220 (293 f.).

Die Vorschriften verstoßen insoweit gegen das allgemeine Persönlichkeitsrecht aus Art. 2 Abs. 1 i.V. mit Art. 1 Abs. 1 GG.

Der Eingriff in das Wohnungsgrundrecht aus Art. 13 Abs. 1 GG ist durch die Schrankenvorbehalte des Art. 13 Abs. 2-7 GG nicht gedeckt, insbesondere ist das Betreten einer Wohnung nicht als Durchsuchung im Sinne des Art. 13 Abs. 2 GG zu verstehen. Insoweit §§ 12, 13 HVSG die Ermächtigung zum Betreten der Wohnung umfassen, sind diese Regelungen folglich auch in Hinblick auf Art. 13 Abs. 1 GG verfassungswidrig.

2. Verfahrensanforderungen

a) Unzureichende Benachrichtigungspflichten

Der Gesetzgeber muss nach der Rechtsprechung des angerufenen Gerichts Ermächtigungen zu eingriffsintensiven verdeckten Überwachungsmaßnahmen durch Benachrichtigungspflichten flankieren. Aufgrund des verdeckten Charakters solcher Maßnahmen dienen die Benachrichtigungspflichten einerseits der Gewährleistung subjektiven Rechtsschutzes im Sinne des Art. 19 Abs. 4 GG und tragen andererseits zur Verhältnismäßigkeit der Überwachungsermächtigung bei. Das Gesetz kann Ausnahmen von der Benachrichtigungspflicht vorsehen, um bedeutsame Allgemeininteressen oder Rechtsgüter Dritter zu schützen. Solche Ausnahmen sind jedoch auf das unbedingt Erforderliche zu beschränken und müssen dem Gebot der Normenklarheit und Bestimmtheit genügen,

BVerfGE 141, 220 (282 f.).

Das HVSG verfehlt die verfassungsrechtlichen Anforderungen an die nachträgliche Benachrichtigung des Betroffenen für nahezu alle Überwachungsermächtigungen und verletzt die Beschwerdeführer*innen zu 1-5 dadurch in ihrem Grundrecht auf Gewährleistung subjektiven Rechtsschutzes aus Art. 19 Abs. 4 GG. Angesichts der Schwere der durch die jeweiligen Überwachungsermächtigungen ermöglichten Grundrechtseingriffe haben die unzureichenden Benachrichtigungspflichten zudem die Unverhältnismäßigkeit der jeweiligen Ermächtigungen zur Folge und verletzen dadurch die Beschwerdeführer*innen zu 1-5 in ihren Grundrecht auf

informationelle Selbstbestimmung aus Art. 2 Abs. 1 i.V. mit Art. 1 Abs. 1 GG, auf Unverletzlichkeit der Wohnung aus Art. 13 Abs. 1 GG und auf das Fernmeldegeheimnis aus Art. 10 Abs. 1 GG.
Die Ermächtigungen zur Ortung von Mobilfunkendgeräten (§ 9 HVSG) und zum Einsatz von Verdeckten Mitarbeitern (§ 12 HVSG) und Vertrauensleuten (§ 13 HVSG) ermöglichen schwere Grundrechtseingriffe,

vgl. D I 1 b, d.

§§ 9, 12, 13 HVSG sehen jedoch keine Benachrichtigung der Betroffenen vor und sind daher mangelhaft.

In §§ 6 S. 5, 8 Abs. 4, 10 Abs. 6, 11 Abs. 9 HVSG sind Benachrichtigung der Betroffenen vorgesehen. Angesichts der Schwere der durch die in Bezug genommenen Überwachungsermächtigungen ermöglichten Eingriffe enthalten diese Regelungen jedoch zu weit gefasste Ausnahmen.

Die Befugnis zur Telekommunikationsüberwachung gemäß § 6 HVSG begründet schwerwiegende Eingriffe in Art 10 Abs. 1 GG,

vgl. BVerfGE 113, 348 (382); 129, 208 (240).

Die in §§ 7, 8 HVSG geregelte Befugnis zur Wohnraumüberwachung ermächtigt den Staat, in Räume einzudringen, die privater Rückzugsort des Einzelnen sind und einen engen Bezug zur Menschenwürde haben. Der Eingriff in Art. 13 Abs. 1 GG ist von besonderer Intensität,

BVerfGE 141, 220 (295).

Die besonderen Auskunftsansprüche in § 10 HVSG stellen, gerade in gebündelter Form, ebenfalls schwerwiegende Eingriffe in das allgemeine Persönlichkeitsrecht dar. Ebenso ermöglicht die Observation gemäß § 11 HVSG gravierende Eingriffe in das allgemeine Persönlichkeitsrecht. Während es die zeitlich begrenzte schlichte Beobachtung noch als mittelschwerer Eingriff einstufte, sah das angerufene Gericht in der langfristig-dauerhaften heimlichen Aufzeichnung von Wort und Bild einer Person einen schwerwiegenden Grundrechtseingriff, insbesondere wenn diese Maßnahmen gebündelt und unter Nutzung moderner Technik durchgeführt werden,

BVerfGE 141, 220 (287).

Diese eingriffsintensiven, verdeckten Überwachungsmaßnahmen sind nicht durch hinreichende Benachrichtigungspflichten flankiert.

§§ 6 S. 5, 10 Abs. 6 HVSG verweisen auf die Benachrichtigungsregelung des § 12 Abs. 1 G 10, §§ 8 Abs. 4, 11 Abs. 9 HVSG kopieren den Wortlaut dieser Norm. Die Regelung des § 12 Abs. 1 G 10 verfehlt jedoch im Kontext der eingriffsintensiven und voraussetzungsarmen Überwachungsermächtigungen des HVSG die verfassungsrechtlichen Anforderungen.

Bereits sehr weit geht der Ausnahmetatbestand in § 12 Abs. 1 Satz 2 Alt. 1 G 10, nach dem So darf die Benachrichtigung unterbleiben, solange eine Gefährdung des Zwecks der Beschränkung nicht ausgeschlossen werden kann. Zwar ist die Sicherung des Überwachungszwecks grundsätzlich ein verfassungsrechtlich tragfähiger Grund, die Benachrichtigung zurückzustellen,

BVerfGE 129, 208 (254); BVerfGE 141, 220 (282 ff).

Indem jedoch §§ 6 S. 5, 8 Abs. 4, 10 Abs. 6, 11 Abs. 9 HVSG die Benachrichtigung generell sperren, solange eine Gefährdung des Überwachungszwecks lediglich nicht auszuschließen ist, lassen diese Normen ihrem Wortlaut nach bereits entfernte Risiken ausreichen, damit der Ausnahmetatbestand greift. Angesichts des weit gefassten Aufklärungsauftrags der Verfassungsschutzbehörden wird sich kaum je mit Sicherheit ausschließen lassen, dass eine Benachrichtigung solche Risiken birgt. Diese Ausnahme beschränkt die Benachrichtigungspflicht daher angesichts der durchweg schweren Grundrechtseingriffe unverhältnismäßig weit. Zumindest bedürfen die Normen einer verfassungskonformen Auslegung, nach der die Benachrichtigung nur ausgeschlossen ist, wenn konkrete Tatsachen für eine Gefährdung des Überwachungszwecks sprechen,

vgl. die einschränkende Auslegung des (deutlich restriktiver gefassten) Ausnahmetatbestands in § 20w Abs. 2 Satz 1 Hs. 2 BKAG durch BVerfGE 141, 220 (320); ferner zu der Vorgängerregelung des heutigen § 12 G 10 BVerfGE 100, 313 (397 f.).

Unverhältnismäßig und auch keiner verfassungskonformen Auslegung zugänglich ist der Ausschluss der Benachrichtigung, solange der Eintritt übergreifender Nachteile für das Wohl des Bundes oder eines Landes absehbar ist.

Sowohl der Begriff des Bundes- oder Landeswohls als auch der Begriff der übergreifenden Nachteile sind weitgehend unbestimmt und grenzen den Grund für eine Zurückstellung der Benachrichtigung praktisch nicht ein. Letztlich lässt sich unter das Wohl des Bundes oder eines Landes – anders als unter den etwa in § 20w Abs. 2 Satz 1 BKAG genannten Bestand des Staates – der gesamte Aufgabenkreis des Landesamts für Verfassungsschutz oder auch jeder anderen Behörde subsumieren,

vgl. zur Interpretation dieses Begriffs im Rahmen von § 96 StPO Ritzert, in: BeckOK StPO, § 96 Rn. 4: „Der Begriff des Nachteils für das Staatswohl wird weit gefasst und ist bereits gegeben, wenn die Erfüllung öffentlicher Aufgaben ernstlich gefährdet oder erheblich erschwert würde".

Zudem müssen die befürchteten Nachteile nach dem Wortlaut der §§ 6 S. 5, 8 Abs. 4, 10 Abs. 6, 11 Abs. 9 HVSG in keinem Zusammenhang mit dem Überwachungszweck stehen, so dass der Ausnahmetatbestand auch hierdurch nicht konkretisiert wird.
Für die Zurückstellung und den endgültigen Ausschluss der Benachrichtigung reichen damit annähernd beliebige behördliche Opportunitätserwägungen aus, solange diese aufgrund einer normativ nicht angeleiteten Abwägung wichtiger erscheinen als die Benachrichtigung.
Für die Verfassungsmäßigkeit dieser Ausnahmeregelungen lässt sich nicht anführen, dass diese Ausschlusstatbestände weitgehend wörtlich dem Urteil des angerufenen Gerichts zur strategischen Telekommunikationsüberwachung nach dem G 10 vom 14. Juli 1999 entnommen sind,

vgl. BVerfGE 100, 313 (398).

Das Bundesverfassungsgericht ist keine Rechtsetzungsinstanz, sondern dazu berufen, grundrechtliche Grenzen der Rechtsetzung zu bestimmen. Es kann sinnvoll oder sogar angezeigt sein, im Rahmen verfassungsgerichtlicher Entscheidungen allgemeine, nicht notwendigerweise unmittelbar subsumtionsfähige Formulierungen zu wählen, um so gesetzgeberische Regelungsspielräume offenzuhalten. Hingegen besteht die Aufgabe des Gesetzgebers darin, diese Regelungsspielräume durch einfaches Recht auszufüllen und so die Verfassung zu konkretisieren. Er kann sich dieser Aufgabe zumindest nicht in jedem Fall dadurch entziehen, dass er Formulierungen aus der Rechtsprechung des Bundesverfassungsgerichts schlicht abschreibt. Insbesondere wäre es sowohl möglich als auch geboten gewesen, den Ausnahmetatbestand zum Schutz des Staatswohls näher zu spezifizieren und auf hinreichend gewichtige Ausnahmegründe zu beschränken. Hierbei hätten auch spezifisch nachrichtendienstliche Belange wie etwa der Quellenschutz oder die Erhaltung von Austauschbeziehungen mit ausländischen Diensten benannt werden können, soweit diese eine Ausnahme von der Benachrichtigungspflicht rechtfertigen können,

> vgl. mit Blick auf die strategische Telekommunikationsüberwachung die beispielhafte Aufzählung bei BVerfGE 100, 313 (398).

b) Auskunftsrechte gemäß § 26 HVSG

Die Regelung über den Auskunftsanspruch des Betroffenen in Art. 26 HVSG genügt ebenfalls nicht in jeder Hinsicht den verfassungsrechtlichen Anforderungen, da das Gesetz den Auskunftsanspruch an zu hohe Anforderungen knüpft und zu weitgehend beschränkt.
Der Auskunftsanspruch des Betroffenen über ihn betreffende Datenverarbeitungen ist das grundlegende Datenschutzrecht,

> statt aller Worms, in: Wolff/Brink (Hrsg.), Datenschutzrecht in Bund und Ländern, 2013, § 19 BDSG Rn. 1.

Das angerufene Gericht hat insbesondere die zentrale Bedeutung dieses Anspruchs für den Grundrechtsschutz betont, wenn eine staatliche Stelle – wie das Landesamt für Verfassungsschutz – zu Informationseingriffen befugt ist, deren Vornahme oder Umfang der Betroffene nicht sicher abschätzen kann, da er in den Informationsverarbeitungsprozess nicht oder nicht stets einbezogen wird, und wenn zudem keine (durchgängige) Pflicht dieser Stelle zur aktiven Benachrichtigung des Betroffenen von Eingriffsmaßnahmen besteht,

> BVerfGE 120, 351 (364).

Gerade in solchen Fallkonstellationen bestehen hohe Anforderungen an Einschränkungen des Auskunftsanspruchs. Eine Einschränkung muss gegenläufigen Interessen von höherem Gewicht dienen. Die gesetzlichen Ausschlusstatbestände müssen sicherstellen, dass die betroffenen Interessen einander umfassend und auch mit Blick auf den Einzelfall zugeordnet werden,

> BVerfGE 120, 351 (365); 133, 277 (367 f.); BVerfGE 141, 220 (283).

Der in Art. 26 HVSG geregelte Auskunftsanspruch ist nach diesen Maßstäben in dreierlei Hinsicht defizitär, indem er eine Auskunftsversagung ohne Rücksicht auf die Umstände des Einzelfalls vorsieht:

Erstens hat der Betroffene gemäß Art. 26 Abs. 1 HVSG einen gebundenen Auskunftsanspruch nur, wenn er „ein besonderes Interesse an einer Auskunft darlegt“. Damit wird dem Betroffenen eine Darlegungslast auferlegt, die mit der Transparenzvorstellung nicht vereinbar ist, welche dem Recht auf informationelle Selbstbestimmung zugrunde liegt. Der Auskunftsanspruch soll dem Betroffenen gerade ermöglichen, sich darüber zu orientieren, wer was über ihn weiß und welche Folgen dieses Wissen für ihn haben kann. Die vorgesehene Darlegungslast führt hingegen dazu, dass der Betroffene bereits – zumindest ansatzweise – über eine solche Orientierung verfügen muss, da er sonst kein „besonderes“ Auskunftsinteresse begründen kann. Schlimmstenfalls kann der Betroffene seinen Auskunftsanspruch nur geltend machen, wenn er das Landesamt selbst auf gegen ihn bestehende Verdachtsmomente hinweist, die sein Auskunftsinteresse begründen,

> drastische, in der Sache aber zutreffende Kritik hieran bei Kauß/Werkentin, KJ 1991, S. 492 (496): „Verpflichtung zur Selbstdenunziation“.

Ein grundrechtlich anerkanntes Auskunftsinteresse ergibt sich vielmehr bereits daraus, dass der Auskunftbegehrende möglicherweise Betroffener von Eingriffen in sein Recht auf informationelle Selbstbestimmung ist. Ein weitergehendes besonderes Interesse kann nur gefordert werden, wenn sich das Auskunftsinteresse des Betroffenen gegen kollidierende staatliche Geheimhaltungsbelange durchsetzen muss. Eine solche Kollisionslage, die mit einer Einzelfallabwägung zu bewältigen wäre, setzt § 26 Abs. 1 Satz 1 HVSG jedoch nicht voraus. Das verfassungsrechtliche Defizit dieser Norm wird im Übrigen nicht dadurch ausgeglichen, dass der Betroffene, wenn er kein besonderes Auskunftsinteresse darlegt, immerhin aus § 23 Abs. 1 Satz 2 HVSG einen Anspruch auf ermessensfehlerfreie Entscheidung über sein Auskunftsbegehren hat. Für ein behördliches Auskunftsermessen ist verfassungsrechtlich jedenfalls dann kein Raum, wenn der Auskunftsanspruch sich auf typischerweise für den Betroffenen nicht vollständig abschätzbare Datenverarbeitungsprozesse bezieht,

> vgl. BVerfGE 120, 351 (364).

Zweitens erstreckt sich die Auskunft nach § 26 Abs. 1 Satz 3 Nr. 1 HVSG von vornherein nicht auf die Herkunft personenbezogener Daten und die Empfänger von Übermittlungen. Gerade diese Angaben können aber für den Betroffenen besonders wichtig sein, um seine informationelle Stellung einzuschätzen. Dies gilt gerade für Auskunftsbegehren gegen Verfassungsschutzbehörden. Diese Behörden müssen seit 2015 miteinander einen umfassenden bundesweiten Informationsverbund unterhalten,

> näher Bergemann, NVwZ 2015, S. 1705 f.

Zudem sind sie mit zahlreichen anderen Sicherheitsbehörden eng vernetzt, insbesondere auch in ständigen Kooperationen wie in den sogenannten gemeinsamen Zentren,

> vgl. zu dem Zentrenmodell und den damit verbundenen verfassungsrechtlichen Problemen den Bericht der Regierungskommission zur Überprüfung der Sicherheitsgesetzgebung in Deutschland vom 28. August 2013, S. 165 ff.

Damit der Auskunftsanspruch des Betroffenen gegenüber einer Verfassungsschutzbehörde seine grundrechtlich gewährleistete Orientierungswirkung entfalten kann, muss er deshalb grundsätzlich Auskünfte über Informationsflüsse zu der und von der Behörde umfassen. Geheimhaltungsinteressen können einer solchen Auskunft im Einzelfall entgegenstehen und sind

dann im Rahmen einer einzelfallbezogenen Abwägung abzuarbeiten, wie sie die Ausschlussgründe in § 26 Abs. 2 HVSG vorsehen,

> vgl. ausdrücklich mit Blick auf Datenbestände von Sicherheitsbehörden BVerfGE 120, 351 (375 f.).

Ein genereller Vorrang des Geheimhaltungsinteresses hinsichtlich der in § 26 Abs. 1 Satz 3 Nr. 1 HVSG genannten Informationen, der einen einzelfallunabhängigen Anspruchsausschluss rechtfertigen könnte, besteht hingegen nicht. Drittens erstreckt sich der Auskunftsanspruch gemäß § 26 Abs. 1 Satz 3 Nr. 2 HVSG nicht auf Daten, die nicht strukturiert in automatisierten Dateien gespeichert sind, es sei denn, der Betroffene macht Angaben, die das Auffinden der Daten ermöglichen, und der für die Erteilung der Auskunft erforderliche Aufwand steht nicht außer Verhältnis zu dem vom Betroffenen geltend gemachten Informationsinteresse. Der prinzipielle Anspruchsanschluss für Daten außerhalb strukturierter Dateien reicht zu weit, weil unter heutigen informationstechnischen Bedingungen insbesondere auch unstrukturierte elektronische Datenbestände (etwa elektronische Akten) mit einer Volltextsuche umfassend erschlossen werden können. Selbst für den Fall einer möglichen Volltextrecherche hat das Bundesverwaltungsgericht einen Auskunftsanspruch über Daten, die in Akten enthalten sind, in verfassungskonformer Auslegung des § 15 BVerfSchG a.F. für begründet erachtet,

> BVerwGE 130, 29.

Jedenfalls soweit das Landesamt seine Datenbestände zur Erfüllung seiner Aufgaben selbst elektronisch in solcher Weise erschließen darf, muss auch der Auskunftsanspruch ohne Weiteres bestehen. Ansonsten würde der Betroffene den Risiken, welche die heutigen Möglichkeiten der Informationsverarbeitung für seine Persönlichkeitsrechte mit sich bringen, in weitem Umfang ausgesetzt, ohne dies wenigstens durch eine Nutzung dieser Möglichkeiten zugunsten des Persönlichkeitsschutzes zu kompensieren. Im Zusammenhang mit elektronisch geführten und informationstechnisch erschließbaren Datenbeständen kann dem Betroffenen auch nicht zugemutet werden, über seine Identität hinaus zusätzliche „Angaben“ zu machen. Denn so wird er ohne sachlichen Grund zur Preisgabe von Informationen gezwungen, die gegebenenfalls wiederum gegen ihn verwendet werden könnten. Schließlich geht es im Zusammenhang mit solchen Datenbeständen nicht an, den Auskunftsanspruch von einer Abwägung zwischen dem Informationsinteresse des Betroffenen und dem mit der Auskunftserteilung verbundenen Aufwand abhängig zu machen. Es ist vielmehr Sache des Landesamts, seine Datenverarbeitungen von vornherein auf den Schutz des Persönlichkeitsrechts einzurichten und zu gewährleisten, dass die Auskunft mit vertretbarem Aufwand erteilt werden kann.

3. Datenverarbeitung und Datenübermittlung

a) Unzureichende Beschränkung der Datenverarbeitung aus Wohnraumüberwachung und Zugriffen auf informationstechnische Systeme, §§ 16, 18 Abs. 3 HVSG

§§ 16, 18 Abs. 3 HVSG verfehlen in Bezug auf die Weiterverarbeitung von übermittelten Daten aus Wohnraumüberwachung und Zugriffen auf informationstechnische Systeme die ver-

fassungsrechtlichen Anforderungen an die Zweckänderung und verletzen die Beschwerdeführer*innen in ihrem Grundrecht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 i.V. mit Art. 1 Abs. 1 GG und ihrem Wohnungsgrundrecht aus Art. 13 Abs. 1 GG.

Die weitere Nutzung und Übermittlung staatlich erhobener Daten richten sich nach den Grundsätzen der Zweckbindung und Zweckänderung. Unter Beachtung der Grundsätze der Zweckbindung kann der Gesetzgeber eine weitere Nutzung der Daten im Rahmen der für die Datenerhebung maßgeblichen Zwecke vorsehen. Eine weitere Nutzung ist danach nur seitens derselben Behörde, im Rahmen derselben Aufgabe und für den Schutz derselben Rechtsgüter möglich. Für Daten aus Wohnraumüberwachungen und Zugriffen auf informationstechnische Systeme ist die Behörde darüber hinaus auch an die Eingriffsschwelle gebunden,

BVerfGE 141, 220 (326).

Eine Nutzung der Daten zu anderen Zwecken, beispielsweise durch eine andere Behörde, unterliegt den Anforderungen an eine Zweckänderung und ist an den Grundrechten zu messen, die für die Datenerhebung maßgeblich waren. Auch hier gilt jedoch nach dem Grundsatz der hypothetischen Datenneuerhebung, dass Daten aus Wohnraumüberwachung und dem Zugriff auf informationstechnische Systeme angesichts des besonderen Eingriffsgewichts auch selbst durch eine dringende Gefahr oder eine im Einzelfall hinreichend konkretisierte Gefahr gerechtfertigt sein müssen,

BVerfGE 141, 220 (329)

§§ 16, 18 HVSG verfehlt diese verfassungsrechtlichen Anforderungen insoweit als diese Norm auch den Empfang und die Nutzung von Daten erfassen, die aus der Wohnraumüberwachung oder dem Zugriff auf informationstechnische Systeme stammen. § 16 HVSG enthält eine Neuregelung der Anforderungen an die Speicherung, Berichtigung, Löschung und Verarbeitung personenbezogener Daten. Umfasst sind von der Regelung nicht nur die vom Landesamt eigens erhobenen Daten, sondern auch Daten, die dem Landesamt durch andere Stellen übermittelt wurden. § 18 HVSG sieht eine Informationsübermittlung durch öffentliche Stellen an das Landesamt vor, wenn tatsächliche Anhaltspunkte dafür bestehen, dass die Informationen für die Erfüllung der Aufgaben des Landesamts erforderlich sein könnten. Neu ist, dass die in § 18 Abs. 1 HVSG aufgezählten Behörden und sonstigen öffentlichen Stellen des Landes zur Übermittlung von Daten verpflichtet sind, wenn die Daten zur Erfüllung der Aufgaben des Landesamts erforderlich sind. Für repressiv erhobene Daten aus Telekommunikationsüberwachungen einschließlich des Zugriffs auf informationstechnische Systeme gemäß § 100 a StPO sieht § 18 Abs. 3 HVSG besondere Beschränkungen für die Übermittlung und Weiterverarbeitung vor. Entsprechende Beschränkungen für übermittelte Daten aus Wohnraumüberwachungen und Online-Durchsuchungen enthält § 18 Abs. 3 HVSG nicht. Auch § 16 HVSG enthält keine Beschränkungen für die Speicherung und Weiterverarbeitung personenbezogener Daten aus Wohnraumüberwachungen und Online-Durchsuchungen. Bezüglich der Nutzung der vom Landesamt selbst erhobenen Daten aus Wohnraumüberwachungen sind entsprechende Vorgaben zur Zweckbindung jedoch in § 8 Abs. 6 HVSG zu finden, der die Speicherung und Weiterverarbeitung personenbezogener Daten aus der Wohnraumüberwachung gemäß § 7 HVSG auf eine im Einzelfall hinreichend konkretisierte Gefahr beschränkt. Für die Speicherung und Nutzung übermittelter Daten aus Wohnraumüberwachungen und Online-Durchsuchungen fehlt es an entsprechenden Beschränkungen.

Da mit dem angegriffenen Gesetz zur Neuausrichtung des Verfassungsschutzes in Hessen die zunächst für den Verfassungsschutz vorgesehenen Ermächtigungen zum Zugriff auf informationstechnische Systeme schließlich im HSOG verankert wurde, gewinnt die Möglichkeit der Übermittlung von Daten aus der Onlinedurchsuchung ans Landesamt eine neue Relevanz,

> vgl. zur Entscheidung des Gesetzgebers, dem Landesamt keine Kompetenz zum Zugriff auf informationstechnische Systeme zu verschaffen, Hessischer Landtag Drs. 19/6502, Seite 22.

Grundsätzlich steht der Zweckänderung zwar nach der Rechtsprechung des angerufenen Gerichts nicht entgegen, dass die empfangende Behörde nicht die Ermächtigungsgrundlagen zur Erhebung dieser Daten besitzt. Das Erfordernis einer Gleichgewichtigkeit der neuen Nutzung bleibt hierdurch jedoch unberührt,

> BVerfGE 141, 220 (328).

Angesichts des besonderen Eingriffsgewichts der Wohnraumüberwachung und des Zugriffs auf informationstechnische Systeme muss jede neue Nutzung der auf diese Weise erhobenen Daten wiederum durch eine dringende Gefahr oder eine im Einzelfall hinreichend konkretisierte Gefahr gerechtfertigt sein,

> BVerfGE 141, 220 (329).

Die Zweckbindung der übermittelnden Daten wird nicht dadurch gewahrt, dass die übermittelnden Behörden entsprechende Beschränkungen in den jeweiligen Ermächtigungsgrundlagen zur Datenübermittlung an das Landesamt enthalten. Der Grundsatz der Zweckänderung erfordert nach dem Bild einer Doppeltür auf beiden Seiten, der übermittelnden und der empfangenden Behörde, die Normierung verfassungskonformer Übermittlungsvoraussetzungen,

> BVerfGE 130, 151 (184); BVerfGE 141, 220 (333 f.).

Zudem unterliegt nur die Datenübermittlung selbst den jeweiligen Übermittlungsvoraussetzungen der übermittelnden Behörde, nicht aber die Weiterverarbeitung durch das Landesamt gemäß § 16 HVSG. Zur Wahrung des Grundsatzes der Zweckänderung in Bezug auf Daten aus Wohnraumdurchsuchungen und Zugriffen auf informationstechnische Systeme bedarf es daher einer Ergänzung des § 16 HVSG oder des § 18 Abs. 3 HVSG.

b) Informationsübermittlung durch das Landesamt innerhalb des öffentlichen Bereichs gemäß § 20 Abs.1 und Abs. 2 HVSG

Die Ermächtigungen des Landesamts zu Informationsübermittlung innerhalb des öffentlichen Bereichs gemäß § 20 Abs. 1 Nr. 1 und 2 und Abs. 2 Satz 1 Nr. 2, Satz 2 HVSG stehen nicht mit den verfassungsrechtlichen Anforderungen im Einklang und verletzen das allgemeine Persönlichkeitsrecht in seiner Ausprägung als Grundrecht auf informationelle Selbstbestimmung aus Art. 1 Abs. 1 GG i. V. mit Art. 2 Abs. 1 GG sowie hinsichtlich personenbezogener Daten aus der Wohnraum- oder Telekommunikationsüberwachung das Grundrecht auf Unverletzlichkeit der Wohnung aus Art. 13 Abs. 1 GG und das Fernmeldegeheimnis aus Art. 10 Abs. 1 GG.

(1) Verfassungsrechtliche Anforderungen

Das angerufene Gericht hat in seinem Urteil zum Antiterrordateigesetz aus dem Recht auf informationelle Selbstbestimmung hohe Anforderungen an Datenübermittlungen von Nachrichtendiensten an Behörden mit operativen Eingriffsbefugnissen errichtet. Zu beurteilen waren seinerzeit insbesondere Datenübermittlungen an Polizei- und Strafverfolgungsbehörden. Für das Verhältnis der Nachrichtendienste zu diesen Behörden hat das Bundesverfassungsgericht ein informationelles Trennungsprinzip errichtet.
Der Grund hierfür liegt in den unterschiedlichen Aufgaben dieser Behörden, denen unterschiedliche Verteilungen von Datenerhebungs- und Zwangsbefugnissen zugrunde liegen. Bei einer Datenübermittlung von einem Nachrichtendienst an eine Polizei- oder Strafverfolgungsbehörde wirken die weitreichenden Datenerhebungsbefugnisse der Nachrichtendienste mit den weitreichenden operativen Zwangsbefugnissen der Polizei- und Strafverfolgungsbehörden zusammen. Hierin liegt ein besonders schwerer Grundrechtseingriff.
Dieser Eingriff genügt nur dann dem Verhältnismäßigkeitsgrundsatz, wenn er einem herausragenden öffentlichen Interesse dient. Dies muss durch eine hinreichend konkrete und qualifizierte Eingriffsschwelle gesichert sein,

> BVerfGE 133, 277 (329).

In seinem Urteil zum BKA-Gesetz hat das angerufene Gericht dieses Erfordernis allgemeingültig für die Zweckänderung, die in einer Datenübermittlung liegt, präzisiert: Danach muss die neue Nutzung der Daten dem Schutz von Rechtsgütern oder der Aufdeckung von Straftaten eines solchen Gewichts dienen, die verfassungsrechtlich ihre Neuerhebung mit vergleichbar schwerwiegenden Mitteln rechtfertigen könnten. Zudem muss sich aus den Daten im Zeitpunkt der Übermittlung ein konkreter Ermittlungsansatz ergeben,

> BVerfGE 141, 220 (328 ff.).

Es ist Aufgabe des Gesetzgebers der Übermittlungsermächtigung, eine Eingriffsschwelle festzulegen, die den verfassungsrechtlichen Anforderungen genügt. Denn dieser Gesetzgeber trägt eine grundrechtliche Regelungsverantwortung für den Umgang mit den Daten, die er zur Erhebung und dann zur Übermittlung freigibt,

> vgl. BVerfGE 125, 260 (346); 130, 151 (201).

Die Übermittlungsermächtigungen in § 20 Abs. 1 und Abs. 2 HVSG werden den verfassungsrechtlichen Anforderungen, die sich aus der jüngeren Rechtsprechung des angerufenen Gerichts ergeben, nicht durchweg gerecht, da sie in erheblichen Teilen zu weit gefasst sind.

(2) Sonderregelung für Übermittlungen an besondere Vollzugsbehörden, § 20 Abs. 2 Satz 1 Nr. 2 HVSG

§ 20 HVSG unterscheidet hinsichtlich der Übermittlungsschwelle zwischen Daten, die mit nachrichtendienstlichen Mitteln erhoben wurden, und sonstigen (insbesondere aus öffentlichen Quellen gewonnenen) Daten des Landesamts. Dies ist eine tragfähige Differenzierung,

> näher zu der unterschiedlichen Eingriffsintensität in beiden Übermittlungskonstellationen Gazeas, Übermittlung nachrichtendienstlicher Erkenntnisse an Strafverfolgungsbehörden, 2014, S. 249 ff.

Für die sensibleren Daten, die mit nachrichtendienstlichen Mitteln erhoben wurden, enthält das Gesetz unterschiedliche Übermittlungstatbestände je nachdem, ob die Daten an die in § 20 Abs. 2 Satz 1 HVSG genannten besonderen Vollzugsbehörden oder an andere Behörden übermittelt werden sollen. Die in § 20 Abs. 2 Satz 1 Nr. 1 und 3 HVSG enthaltenen Übermittlungsermächtigungen werden nicht gerügt. Zu weit und daher verfassungswidrig sind hingegen sämtliche Übermittlungstatbestände in § 20 Abs. 2 Satz 1 Nr. 2 HVSG.

Soweit diese Regelung eine Informationsübermittlung zur *Verfolgung* von Straftaten von erheblicher Bedeutung vorsieht, ist sie deshalb unzureichend, weil der Begriff der Straftat von erheblicher Bedeutung nur unzureichend konkretisiert und begrenzt wird. Nach § 20 Abs. 2 Satz 2 sind unter Straftaten von erheblicher Bedeutung Verbrechen und schwerwiegende Vergehen zu verstehen, wenn die Straftat im Einzelfall mindestens dem Bereich der mittleren Kriminalität zuzurechnen ist, sie den Rechtsfrieden empfindlich stört und dazu geeignet ist, das Gefühl der Rechtssicherheit der Bevölkerung erheblich zu beeinträchtigen.

Nach gängiger Auffassung im strafprozessrechtlichen Schrifttum können als Straftaten von erheblicher Bedeutung bereits Delikte aus dem Bereich der mittleren Kriminalität mit einer Strafobergrenze von zwei Jahren anzusehen sein,

> vgl. etwa zu § 98a StPO Ritzert, in: BeckOK-StPO, § 98a Rn. 1: schon Vergehen mit einer Strafrahmenobergrenze über zwei Jahren, wovon dann auch Delikte wie der Landfriedensbruch oder das unerlaubte Entfernen vom Unfallort umfasst wären.

Für die Einbeziehung von Straftaten mit einer Strafobergrenze von unter fünf Jahren spricht auch die explizite Nennung schwerwiegender Vergehen in der Definition in § 20 Abs. 2 Satz 2 HVSG. Die Konkretisierung auf Straftaten, die geeignet sind, den Rechtsfrieden empfindlich zu stören und das Gefühl der Rechtssicherheit der Bevölkerung erheblich zu beeinträchtigen trägt nicht zur Bestimmbarkeit der erfassten Straftaten bei. Sowohl der Rechtsfrieden als auch die Rechtssicherheit der Bevölkerung sind konturlose, unbestimmte Begriffe, die im Zweifel auch schon bei Aktionen des sozialen Ungehorsams wie Baumbesetzungen oder bei versammlungsspezifischen Straftaten, zB der Blockade einer Versammlung gemäß § 21 VersG bemüht werden können.

Da auf der Grundlage von § 20 Abs. 2 Satz 1 Nr. 2 HVSG auch Informationen übermittelt werden können, die mit eingriffsintensiven nachrichtendienstlichen Mitteln wie etwa längerfristigen Bild- und Tonaufzeichnungen außerhalb von Wohnungen oder dem personengerichteten Einsatz eines verdeckten Ermittlers gewonnen wurden, reicht diese Eingriffsschwelle nicht durchweg aus, um die Übermittlung zu rechtfertigen,

> vgl. zu dem insoweit gleichlautenden § 19 BVerfSchG Bergemann, NVwZ 2015, S. 1705 (1707 f.).

Vielmehr müssen die Straftaten, zu deren Verfolgung die Übermittlung ermöglicht werden soll, so schwer wiegen, dass die übermittelten Informationen auch auf der Grundlage einer strafprozessualen Ermächtigung erlangt werden könnten. Unerheblich ist insoweit, ob die Informationen strafprozessual als Beweismittel oder lediglich als Spurenansatz verwendet werden sollen,

> BVerfGE 141, 220 (315).

Soweit § 20 Abs. 2 Satz 1 Nr. 2 HVSG eine Informationsübermittlung auch zur *Verhinderung* oder zur *sonstigen Verhütung* von Straftaten von erheblicher Bedeutung ermöglicht, vertiefen sich die verfassungsrechtlichen Bedenken noch. Hierfür gibt es zwei Gründe:
Erstens droht der strafprozessuale Begriff der Straftat von erheblicher Bedeutung diesen präventiv ausgerichteten Übermittlungstatbestand zu entgrenzen. Wenn durch eine Straftat Schäden für besonders bedeutsame Rechtsgüter konkret drohen, ist bereits der Übermittlungstatbestand des § 20 Abs. 2 Satz 1 Nr. 1 HVSG verwirklicht. Einer weiteren Übermittlungsermächtigung, die spezifisch auf die Kriminalprävention zugeschnitten ist, bedarf es insoweit nicht. Allerdings finden sich im materiellen Strafrecht zahlreiche Deliktstatbestände, die Handlungen im Vorfeld strafbarer Rechtsgutsverletzungen bei Strafe verbieten. Insbesondere das Terrorismusstrafrecht zeichnet sich durch eine nahezu flächendeckende Vorfeldkriminalisierung aus. Viele dieser Straftaten sind schon wegen hoher Strafandrohungen ohne weiteres als Straftaten von erheblicher Bedeutung anzusehen, die im strafrechtlichen Ermittlungsverfahren eingriffsintensive Überwachungsmaßnahmen rechtfertigen können, wenn ein Tatverdacht besteht,

> vgl. beispielhaft § 89a StGB (Vorbereitung einer schweren staatsgefährdenden Gewalttat) – Freiheitsstrafe von sechs Monaten bis zu zehn Jahren; § 129 StGB (Bildung krimineller Vereinigungen) - Freiheitsstrafe bis zu fünf Jahren; § 129a Abs. 1 und 2 StGB (Bildung einer terroristischen Vereinigung) – Freiheitsstrafe von einem Jahr bis zu zehn Jahren.

Wird jedoch der materiell-strafrechtliche Vorfeldansatz mit den Regelungsmustern präventivpolizeilicher Eingriffsermächtigungen verbunden, so droht der Eingriffsanlass zu entgrenzen, indem die strafrechtliche Vorverlagerung noch ausgedehnt wird.

Soweit ein eigenständiger Übermittlungstatbestand für Zwecke der polizeilichen Kriminalprävention in § 20 Abs. 2 Satz 1 HVSG überhaupt erforderlich sein sollte, hätten die Straftaten, die eine Datenübermittlung rechtfertigen, nach spezifisch präventivpolizeilichen Kriterien ausgewählt und enumerativ aufgezählt werden müssen. Nur so hätte der Gesetzgeber gewährleisten können, dass der Übermittlung in jedem Fall ein verfassungsrechtlich hinreichender Ermittlungsansatz zugrunde liegt.

(3) Informationsübermittlung wegen Staatsschutzdelikten, § 20 Abs. 2 Satz 3 HVSG

Gleichfalls zu weit gefasst ist die Übermittlungsermächtigung in § 20 Abs. 2 Satz 3 HVSG mit ihrem Verweis auf § 20 BVerfSchG.
Nach diesen Normen muss das Landesamt Informationen an die Polizei- und Strafverfolgungsbehörden übermitteln, wenn sie benötigt werden, um Staatsschutzdelikte zu verhindern oder zu verfolgen. Der damit maßgebliche Begriff des Staatsschutzdelikts wird in § 20 Abs. 1 Satz 2 BVerfSchG definiert. Er reicht viel zu weit und umfasst bei entsprechender Motivation des Täters auch Straftaten von geringem Gewicht wie eine Beleidigung oder Sachbeschädigung, deren Verhinderung oder Verfolgung die Übermittlung von Daten nicht rechtfertigen kann, die aus eingriffsintensiven Überwachungsmaßnahmen stammen. Nur am Rande sei angemerkt, dass andererseits keine Übermittlungspflicht bei Straftaten ohne Staatsschutzbezug besteht, selbst wenn es sich um schwerste Kriminalität handelt,

eingehend zu den Bedenken gegen § 20 BVerfSchG Gazeas, Übermittlung nachrichtendienstlicher Erkenntnisse an Strafverfolgungsbehörden, 2014, S. 318 ff.

(4) Allgemeine Übermittlungsermächtigung, § 20 Abs. 1 HVSG

Gegen die allgemeine Übermittlungsermächtigung in § 20 Abs. 1 HVSG werden insoweit keinen verfassungsrechtlichen Bedenken vorgebracht, als sie eine Übermittlung von Informationen ermöglicht, die das Landesamt ohne Rückgriff auf nachrichtendienstliche Mittel – insbesondere also durch die Auswertung öffentlich zugänglicher Quellen – erlangt hat. Der Gesetzgeber darf der geringeren Eingriffsintensität einer solchen Informationserhebung Rechnung tragen, indem die Anforderungen an eine Übermittlung der Informationen gleichfalls abgesenkt werden.

Verfassungswidrig ist § 20 Abs. 1 HVSG jedoch insoweit, als diese Norm unter niedrigen Voraussetzungen ausdrücklich eine Übermittlung auch von solchen Informationen zulässt, die mit nachrichtendienstlichen Mitteln gewonnen wurden:

§ 20 Abs. 1 Nr. 1 HVSG erlaubt eine Übermittlung solcher Informationen generell für Zwecke der öffentlichen Sicherheit. Da der Begriff der öffentlichen Sicherheit die Integrität der gesamten Rechtsordnung umfasst und fast jede Behörde berufen ist, zur Wahrung der Rechtsordnung beizutragen, wird so eine Übermittlung an nahezu beliebige Empfangsbehörden außerhalb des Anwendungsbereichs des Abs. 2 ermöglicht, wenn die Übermittlung nur nützlich sein kann, damit diese Behörden ihre Aufgaben erfüllen können. Eine qualifizierte Übermittlungsschwelle hinsichtlich der zu schützenden Rechtsgüter oder des Übermittlungsanlasses fehlt auch für Informationen, die aus eingriffsintensiven Maßnahmen wie längerfristigen Film- und Tonaufzeichnungen außerhalb von Wohnungen oder dem Einsatz von verdeckten Ermittlern stammen.

Dieser Regelung liegt ein zu enges Verständnis der Feststellungen zugrunde, die das angerufene Gericht in seinem Urteil zur Antiterrordatei getroffen hat. Das angerufene Gericht hatte sich dort – entsprechend dem Zuschnitt der Antiterrordatei – unmittelbar allein mit einem Datenaustausch zwischen Nachrichtendiensten einerseits und Polizei- und Strafverfolgungsbehörden andererseits zu befassen. Dementsprechend hat es das informationelle Trennungsprinzip ausdrücklich auf das Verhältnis dieser Behörden zueinander bezogen. Daraus lässt sich jedoch nicht folgern, dass hohe Übermittlungsschranken nur im Verhältnis der Nachrichtendienste zu Empfangsbehörden mit spezifisch polizeilichen Zwangsbefugnissen bestehen,

zumindest in diese Richtung jedoch die Gesetzesbegründung, LT-Drs.19/5412, Seite 47.

Vielmehr muss der Ableitungszusammenhang des informationellen Trennungsprinzips einbezogen werden,

BVerfGE 133, 277 (324 ff.).

Die Ausführungen des angerufenen Gerichts gehen von den unterschiedlichen Aufgaben und Befugnissen der Nachrichtendienste einerseits und der anderen behandelten Behörden andererseits aus. Eine Datenübermittlung von einem Nachrichtendienst an eine andere Behörde bewirkt dann und deshalb einen besonders schweren Grundrechtseingriff, wenn dadurch die weitreichenden Befugnisse der Nachrichtendienste zu verdeckten Informationserhebungen mit weitreichenden Befugnissen zu imperativen Grundrechtseingriffen verbunden werden. Dem-

entsprechend nennt das Urteil als Behörden, deren Tätigkeit grundlegend anders zugeschnitten ist als die der Nachrichtendienste, neben Polizeibehörden ausdrücklich auch (sonstige) Sicherheitsbehörden,

BVerfGE 133, 277 (327).

Diese Erwägungen legen nahe, das informationelle Trennungsprinzip auf das Verhältnis der Nachrichtendienste zu Sonderordnungsbehörden zu übertragen, die gleichfalls über einschneidende imperative Befugnisse verfügen können. So können Eingriffsmaßnahmen von Gewerbeaufsichts- oder Ausländerbehörden aus Sicht der Betroffenen ebenso schwere, mitunter sogar schwerere Folgen haben als Eingriffsmaßnahmen der Polizei oder auch als eine strafrechtliche Verurteilung. Daher leuchtet es nicht ein, dass Informationsübermittlungen an solche Behörden den Nachrichtendiensten ohne signifikante Eingriffsschwelle möglich sein sollen, während Übermittlungen an Polizei- und Strafverfolgungsbehörden als besonders schwere Eingriffe nur ausnahmsweise unter restriktiven Bedingungen zulässig sein können.
Das Urteil zum BKA-Gesetz, welches das – teilweise modifizierte – Regelungskonzept der hypothetischen Datenneuerhebung als verfassungsrechtlich gebotene Vorgabe für Zweckänderungen entfaltet hat, bestätigt diesen Befund. Denn danach muss die Eingriffsschwelle für eine Informationsübermittlung hinsichtlich der geschützten Rechtsgüter den Anforderungen an die Erhebung der Informationen genügen und ist ein hinreichend konkreter Übermittlungsanlass festzulegen,

BVerfGE 141, 220 (287 ff.).

Die in § 20 Abs. 1 Nr. 1 HVSG vorgesehenen Tatbestände können daher eine Übermittlung von Informationen, die mit nachrichtendienstlichen Mitteln gewonnen wurden, zumindest in der Regel nicht legitimieren. Für die Übermittlung solcher Informationen sind generell enger begrenzte Eingriffsschwellen sowohl hinsichtlich der zu schützenden Rechtsgüter als auch hinsichtlich des Übermittlungsanlasses verfassungsrechtlich geboten.

Verfassungswidrig ist daneben auch der noch weiter gefasste § 20 Abs. 1 Nr. 2 HVSG, der Datenübermittlungen auch zur Erfüllung anderer behördlicher Aufgaben erlaubt, wenn die Empfangsbehörde nur „zum Schutz der freiheitlichen demokratischen Grundordnung beizutragen oder Gesichtspunkte der öffentlichen Sicherheit oder auswärtige Belange zu würdigen hat“. Diese Formulierung gibt die Übermittlung von Informationen, die mit nachrichtendienstlichen Mitteln gewonnen wurden, praktisch vollständig frei, da so gut wie jede Behörde berufen ist, die genannten Belange zu beachten.

(5) Auslandsübermittlungen, § 21 Abs. 2 HVSG

Die in § 21 Abs. 2 HVSG enthaltene Ermächtigung zur Informationsübermittlung an ausländische, zwischen- und überstaatliche Stellen steht hinsichtlich von Informationen, die durch den Einsatz eingriffsintensiver nachrichtendienstlicher Mittel gewonnen wurden, gleichfalls nicht mit den verfassungsrechtlichen Anforderungen in Einklang.
Eine Ermächtigung zu Auslandsübermittlungen muss in hinreichend bestimmter und normenklarer Weise den Anforderungen an eine Zweckänderungsermächtigung genügen. Ebenso wie die Übermittlung im Inland ist jedoch auch für die Übermittlung ins Ausland erforderlich, dass die Daten der Aufdeckung vergleichbar gewichtiger Straftaten oder dem Schutz vergleichbar gewichtiger Rechtsgüter dienen, wie sie für die ursprüngliche Datenerhebung maß-

geblich waren. Zudem setzt die Übermittlung einen datenschutzrechtlich angemessenen Umgang mit den übermittelten Daten im Empfängerstaat sowie eine wirksame inländische Kontrolle voraus. Diese Maßgaben müssen in einer den Grundsätzen der Bestimmtheit und Normenklarheit entsprechenden Weise gesetzlich ausgeformt sein,

BVerfGE 141, 220 (329 ff.).

§ 21 Abs. 2 HVSG erfüllt diese Anforderungen nicht. Die Norm ermöglicht eine Übermittlung zur Wahrung unspezifischer „erheblicher Sicherheitsinteressen" des Empfängers, ohne die zu schützenden Rechtsgüter oder den Übermittlungsanlass auch nur ansatzweise zu konkretisieren. Wie das angerufene Gericht zutreffend ausführte, ist die Eigenständigkeit der jeweils anderen Rechtsordnung zu berücksichtigen,

BVerfGE 141, 220 (331).

Doch auch unter Berücksichtigung der ausländischen Rechtsordnungen ist es durchaus möglich, die Übermittlungsvoraussetzungen gesetzlich zu konkretisieren. Dies kann beispielsweise durch den Bezug auf konkrete Rechtsgüter geschehen, die sich unabhängig von der jeweiligen Rechtsordnung einordnen lassen. Nicht ausreichend ist der Hinweis in § 21 Abs. 4 Satz 3 HVSG, dass der Empfänger auf die Verwendungsbeschränkung hinzuweisen ist.

Zu dem gebotenen Kontrollregime findet sich nur der Hinweis in § 21 Abs. 4 Satz 3 HVSG, dass sich das Landesamt vorbehält, Auskünfte über die Verwendung der Daten zu verlangen. Die vom angerufenen Gericht beschriebenen Kontrollmechanismen wie die Abgabe von Einzelgarantien des Empfängerstaates, die Dokumentation der Übermittlung, die Überprüfung durch den Datenschutzbeauftragten und flankierende Berichtspflichten,

BVerfGE 141, 220 (337 ff.)

finden in § 21 HVSG keine Erwähnung.

II. Verfassungswidrigkeit der angegriffenen Regelungen im HSOG

1. Online-Durchsuchung und Quellen TKÜ, §§ 15b, 15c HSOG

Die Ermächtigungen zur Telekommunikationsüberwachung an informationstechnischen Systemen gemäß § 15b HSOG und zum verdeckten Eingriff in informationstechnische Systeme gemäß § 15c HSOG genügen bei einer rein subjektiv-rechtlichen Betrachtung den verfassungsrechtlichen Anforderungen, wie sie das angerufene Gericht in seinem BKAG-Urteil herausgearbeitet hat,

BVerfGE 141, 220 (272 ff.).

§§ 15b, 15c HSOG sind gleichwohl verfassungswidrig, denn sie verletzen die objektivrechtlichen Anforderungen des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (dazu unter a).

Das Land Hessen hätte die genannten Befugnisse mit einem effektiven Schwachstellen-Management verbinden müssen, welches insbesondere die Verwendung von Sicherheitslücken verhindert, die dem Hersteller des betreffenden Systems noch nicht bekannt sind, sog. Zero-Days (dazu unter b).

Die derzeitige Ausgestaltung der §§ 15b, 15c HSOG verletzt die Beschwerdeführer*innen zu 1 bis 7 daher in ihren Grundrechten auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme aus Art. 2 Abs. 1 i.V. mit Art. 1 Abs. 1 GG bzw. Art. 2 Abs. 1 GG. Dieses Grundrecht schützt auch die Beschwerdeführerin zu 7 als juristische Person (dazu unter c).

a) objektivrechtliche Anforderungen des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme

Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme aus Art. 2 Abs. 1 i.V. mit Art. 1 Abs. 1 GG bzw. Art. 2 Abs. 1 GG ist nicht nur ein subjektives Abwehrrecht gegen staatliche Eingriffe. Es begründet – wie schon der Begriff der Gewährleistung zeigt – auch eine staatliche Pflicht dazu beizutragen, dass die Sicherheit der informationstechnischen Infrastruktur der Bundesrepublik ein hohes Niveau erreicht. Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme trägt so einerseits der hohen Bedeutung der Informationstechnik für die Funktionsfähigkeit von Staat und Gesellschaft, andererseits der erheblichen Verwundbarkeit dieser Technologie Rechnung,

> vgl. etwa Sachs/Krings, JuS 2008, 481 (486); Kutscha, NJW 2008, 1042 (1044); Roßnagel/Schnabel, NJW 2008, 3534 (3535); Heckmann, in: FS Käfer, 2009, S. 129 (133 ff.); Hoffmann-Riem, JZ 2009, S. 165 ff.; ders., AöR 134 (2009), S. 513 ff.; ders., JZ 2014, S. 53 ff.; Becker, NVwZ 2015, 1335 (1339 f.).

Die objektiv-rechtliche Dimension des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme ist praktisch hoch bedeutsam, weil solche Systeme strukturell bedingt stets eine Vielzahl von Sicherheitslücken aufweisen, die eigenständig zu Fehlfunktionen führen oder durch Dritte missbräuchlich ausgenutzt werden können. Die Sicherheit informationstechnischer Systeme ist daher als dauerhafte öffentliche Aufgabe anzusehen. Diese Aufgabe kann der Staat allerdings weitgehend nicht eigenhändig erfüllen, da es ihm hierfür sowohl an Ressourcen als auch an Expertise fehlt. In erster Linie obliegt es vielmehr den Herstellern von informationstechnischen Systemen und der darauf laufenden Software, vermeidbare Sicherheitslücken nicht entstehen zu lassen und später erkannte Sicherheitslücken zeitnah zu schließen. Die staatliche Gewalt kann hierbei lediglich eine unterstützende Rolle einnehmen. Welche Beiträge sie dazu übernimmt, hängt von Gestaltungsentscheidungen ab, für die das Grundgesetz beträchtliche Spielräume lässt. Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme ist in seiner objektiv-rechtlichen Dimension erst verletzt, wenn die staatlichen Anstrengungen offenkundig unzureichend sind,

vgl. zu aus unterschiedlichen Grundrechten hergeleiteten staatlichen Schutzpflichten etwa BVerfGE 49, 89 (142); 77, 17 (214 f.); 88, 203 (251 ff.); 92, 26 (46); 106, 28 (37); 125, 39 (78 f.); 143, 313 (337 f.).

Der grundrechtliche Mindeststandard wird allerdings zumindest dann unterschritten, wenn eine staatliche Stelle ohne zureichenden Grund eine Gefährdungslage für die Vertraulichkeit und Integrität der informationstechnischen Infrastruktur in der Bundesrepublik bewusst aufrechterhält oder sogar selbst schafft. Eine solche Situation kann im Zusammenhang mit Online-Durchsuchungen und Quellen-Telekommunikationsüberwachungen abhängig von dem genutzten Infiltrationsweg auftreten. Insbesondere ist dies der Fall, wenn für die Infiltration des Zielsystems eine noch unbekannte Sicherheitslücke von Hardware oder Software ausgenutzt wird (sogenannter Zero-Day).
Da ein Zero-Day dem Hersteller und den Nutzern des betroffenen informationstechnischen Systems noch unbekannt ist, gibt es gegen ihn aus Sicht dieser Personen keine wirksamen Gegenmaßnahmen. Soweit die Sicherheitslücke sich prinzipiell durch eine Anpassung des Systems (etwa ein Software-Update) schließen ließe, steht der dafür erforderliche technische Baustein noch nicht zur Verfügung. Für die ansonsten notfalls mögliche und gebotene vollständige oder partielle Außerbetriebnahme des Systems besteht aus Sicht der betroffenen Personen kein Anlass, solange die Sicherheitslücke nicht bekannt ist.
Sicherheitsbehörden können Zero-Days ausnutzen, um informationstechnische Systeme zu infiltrieren und so eine Online-Durchsuchung oder eine Quellen-Telekommunikationsüberwachung zu ermöglichen. Dieser Infiltrationsweg erzeugt jedoch einen Zielkonflikt zwischen den Sicherheitsbelangen, denen die Maßnahme dient, und dem durch das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität gewährleisteten Anliegen, dass der Staat zur Sicherheit der informationstechnischen Infrastruktur in der Bundesrepublik beiträgt.
Im Sinne der Effektivität der Überwachungsmaßnahme muss die Sicherheitslücke möglichst lange geheim gehalten werden. Wird die Sicherheitslücke bekannt, besteht die Gefahr, dass sie geschlossen wird und darum die Infiltration von vornherein misslingt oder die Maßnahme vorzeitig abgebrochen werden muss. Selbst nach Beendigung der einzelnen Überwachungsmaßnahme besteht ein Interesse daran, den Zero-Day weiterhin geheim zu halten, um ihn für weitere Online-Durchsuchungen oder Quellen-Telekommunikationsüberwachungen nutzen zu können.
Die Ausnutzung von Zero-Days durch staatliche Stellen kann zugleich in mehrfacher Hinsicht die Bedrohungslage für die informationstechnische Infrastruktur in der Bundesrepublik aufrechterhalten oder sogar noch verschärfen.
Wird eine Sicherheitslücke aus den eben genannten Gründen geheim gehalten, so trägt die handelnde Behörde durch ihr Unterlassen dazu bei, dass diese Sicherheitslücke nicht geschlossen wird. Da sich aus technischer Sicht die Infiltration informationstechnischer Systeme durch staatliche Stellen und durch Kriminelle nicht unterscheiden, perpetuiert dieses Unterlassen das Risiko krimineller Übergriffe auf die informationstechnische Infrastruktur.
Einen darüberhinausgehenden Beitrag zur Schwächung der Informationssicherheit in der Bundesrepublik leistet der Staat dann, wenn eine Behörde Informationen über eine Sicherheitslücke nicht selbst generiert, sondern von Dritten bezieht. Dies ist kein unrealistisches Szenario. Noch in jüngerer Zeit hat der Präsident der Zentralen Stelle für Informationstechnik im Sicherheitsbereich („ZITiS“), einer neuen Einrichtung des Bundes, die Sicherheitsbehörden bei der Identifikation und Ausnutzung von Sicherheitslücken unterstützen soll, eingeräumt, seine Stelle verfüge bislang nicht über die technische Expertise, um Sicherheitslücken im benötigten Umfang selbst aufzudecken,

vgl. https://www.heise.de/newsticker/meldung/Schlagabtausch-zu-ZITiS-IT-Sicherheitsluecken-schliessen-oder-ausnutzen-3976587.html, zuletzt abgerufen am 01.07.2019.

Werden Zero-Days auf dem Markt eingekauft, so stützt die beschaffende staatliche Stelle diesen Markt aktiv. Schon wegen der strengen strafrechtlichen Regulierung des Umgangs mit Informationen und Software, die zum Ausspähen oder Abfangen von Daten bestimmt sind (vgl. § 202c StGB), ist anzunehmen, dass die Akteure auf diesem Markt regelmäßig zumindest in einem rechtlichen Graubereich agieren. Die staatliche Unterstützung dieses Marktes birgt darum das erhebliche Risiko, mittelbar Straftaten zu begünstigen. Sie kann zudem zur Stabilisierung des Marktes und zur Vermehrung der angebotenen Sicherheitslücken beitragen, die dann auch von Dritten aufgekauft und ausgenutzt werden können. Im besten Fall konkurrieren die Behörden unmittelbar mit Unternehmen und Sicherheitsdienstleistern um den Ankauf der entsprechenden Informationen, treiben den Preis in die Höhe und schwächen Programme, die mittels monetärer Anreize zur Aufdeckung von Schwachstellen animieren (sog. Bug Bounty).

Eine staatliche Stelle, die über einen geheim gehaltenen Bestand von Informationen über Zero-Days verfügt, ist schließlich selbst ein lohnendes Angriffsziel für Kriminelle, die sich diese Informationen beschaffen und für eigene Zwecke nutzen können. Hierbei handelt es sich nicht um ein hypothetisches Szenario, das als Restrisiko der staatlichen Aufklärung außer Acht bleiben könnte. Solche Angriffe liegen vielmehr ausgesprochen nahe und sind schon vorgekommen.

So hat im Mai 2017 das Schadprogramm „WannaCry“ weltweit erhebliche Schäden verursacht. Dieses Schadprogramm nutzte eine Sicherheitslücke in Windows-Betriebssystemen aus, welche die kriminellen Angreifer nach verbreiteter Einschätzung mitsamt der zugehörigen Angriffswerkzeuge bei der US-amerikanischen National Security Agency (NSA) ausgespäht hatten, die ihrerseits diese Sicherheitslücke für eigene Zwecke eingesetzt und geheim gehalten hatte,

vgl. etwa http://www.zeit.de/digital/internet/2017-05/wannacry-microsoft-nsa-hackerangriff-usa-regierung; https://www.tagesschau.de/ausland/wannacry-107.html, zuletzt abgerufen am 01.07.2019.

Chinesische Spione sollen diese Sicherheitslücke bereits im Jahr 2016 von der NSA erlangt und für eigene Angriffe genutzt haben,

vgl. https://www.nytimes.com/2019/05/06/us/politics/china-hacking-cyber.html, zuletzt abgerufen am 01.07.2019.

Es liegt fern, dass deutsche Sicherheitsbehörden die bei ihnen vorhandenen Informationen über Sicherheitslücken bedeutend besser schützen können als die NSA. Vielmehr ist anzunehmen, dass ein Verlust sich nie ausschließen lässt. Mit vergleichbaren Vorfällen infolge einer Sammlung von Sicherheitslücken bei deutschen Behörden wäre daher zu rechnen.

b) Aufgabe des Landes Hessen bei der Gewährleistung der IT-Sicherheit

Werden die Risiken und die möglichen Erträge der staatlichen Infiltration informationstechnischer Systeme mithilfe von Zero-Days einander gegenübergestellt, so ergibt sich, dass dieser Infiltrationsweg ausgeschlossen werden muss.
Die durch die Nutzung und Geheimhaltung von Zero-Days eröffneten oder zumindest erhöhten Risiken wiegen äußerst schwer.
Zum einen kann der kriminelle Missbrauch der geheim gehaltenen Sicherheitslücken hochrangige Rechtsgüter empfindlich bedrohen. Nahezu alle lebenswichtigen Leistungen werden heute mit informationstechnischer Unterstützung erbracht. Ebenso verfügen so gut wie sämtliche staatlichen und gesellschaftlichen Einrichtungen, deren Ausfall oder Funktionsstörung schwere Schäden verursachen kann, über informationstechnische Komponenten. Werden solche informationstechnischen Komponenten gestört, so kann dies zu Leistungsausfällen oder Schadensereignissen führen, die schlimmstenfalls den Verlust von Menschenleben zur Folge haben können. Beispielsweise hat das oben erwähnte Schadprogramm „WannaCry" informationstechnische Systeme in britischen Krankenhäusern infiltriert. In der Folge mussten unter anderem geplante Operationen verschoben werden. Auch rund 450 Rechner der Deutschen Bahn wurden infiziert, was unter anderem zum Ausfall einer regionalen Leitstelle führte. Ein weiterer Angriff, der auf von der NSA erbeuteter Technologie basierte, führte dazu, dass bei dem Arzneimittelunternehmen Merck ein kritischer Minderbestand eines Impfstoffs eintrat.
Zum anderen erstreckt sich die Bedrohung durch den Missbrauch von Zero-Days auf praktisch die gesamte Bevölkerung, also ganz überwiegend auf Menschen, die für sicherheitsbehördliche Überwachungsmaßnahmen keinen Anlass geben. Es fehlt mithin vollständig an einer Zurechnungsbeziehung zwischen diesen Menschen und den Belangen, die der Geheimhaltung von Sicherheitslücken zugrunde liegen. Angesichts dessen und wegen der drohenden schweren Schäden ist die Grenze der Aufopferungspflicht des Einzelnen für das Gemeinwohl deutlich überschritten.
Hingegen wiegt der Effektivitätsverlust, der durch ein Verbot der Ausnutzung von Zero-Days für die Aufgabenerfüllung der Sicherheitsbehörden droht, weniger schwer. Zwar haben die Belange, denen Online-Durchsuchungen und Quellen-Telekommunikationsüberwachungen des BKA dienen, schon wegen der grundrechtlich gebotenen restriktiven Fassung des Eingriffstatbestands durchweg hohes Gewicht. Jedoch können diese Belange zumeist auch auf weniger riskanten Wegen erreicht werden. So ist es aus objektiv-rechtlicher Sicht beispielsweise unbedenklich, wenn zur Infiltration des Zielsystems einer Online-Durchsuchung bzw. einer Quellen-Telekommunikationsüberwachung eine physische Zugriffsmöglichkeit (etwa im Rahmen einer Durchsuchung) oder eine bereits bekannte, auf diesem System jedoch noch nicht geschlossene Sicherheitslücke ausgenutzt werden. Soweit im Einzelfall eine Infiltration auf solchen Wegen nicht möglich sein sollte, ist der damit verbundene Ausfall dieser Überwachungsmaßnahmen hinzunehmen und auf andere, gegebenenfalls teurere Maßnahmen auszuweichen.
Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme verpflichtet die staatliche Gewalt mithin dazu, auf die Nutzung und Geheimhaltung von Zero-Days zum Zweck der Infiltration informationstechnischer Systeme zu verzichten. Es ist Sache des Gesetzgebers, diese Pflicht durch ein ausdrückliches gesetzliches Verbot umzusetzen. Nur durch ein ausdrückliches Verbot erhalten die Sicherheitsbehörden eine eindeutige Vorgabe, die das objektiv-grundrechtlich nicht hinzunehmende Risiko für die Sicherheit der informationstechnischen Infrastruktur der Bundesrepublik sicher ausschließt.
Dass es einer solchen Vorgabe bedarf, illustriert beispielhaft die Antwort der Bundesregierung auf eine parlamentarische Kleine Anfrage, in der die Bundesregierung eine Nutzung von Zero-Days zumindest nicht ausgeschlossen hat:

„Ob und inwieweit im Spannungsfeld technischer Erfordernisse, rechtlicher Vorgaben, sicherheits- und rechtspolitischer Erwägungen sowie taktischer Einsatzrahmenbedingungen zukünftig eine Nutzung sog. ‚Zero-Day-Exploits' für die Durchführung von Maßnahmen der Quellen-TKÜ und Online-Durchsuchung durch Sicherheitsbehörden in Betracht kommt, ist durch die zuständigen Stellen der Bundesregierung in Abstimmung mit den zu beteiligenden nationalen und ggf. internationalen Stellen und Gremien zu prüfen." Antwort der Bundesregierung auf Fragen 26 bis 31 einer Kleinen Anfrage, BT-Drs. 18/13413; die Antwort auf diese Fragen ist eingestuft, aber online zugänglich unter https://netzpolitik.org/2018/geheime-dokumente-das-bundeskriminalamt-kann-jetzt-drei-staatstrojaner-einsetzen/#Antwort-Drucksache-18-13566-NfD, zuletzt abgerufen am 01.07.2019.

Selbst wenn entgegen der oben begründeten Auffassung eine staatliche Infiltration informationstechnischer Systeme mithilfe von noch unbekannten Sicherheitslücken verfassungsrechtlich überhaupt rechtfertigungsfähig wäre, müsste die gesetzliche Grundlage der Infiltration zumindest Vorgaben für ein behördliches Schwachstellen-Management enthalten. Nur aufgrund prozeduraler Sicherungen und materieller Kriterien für ein solches Schwachstellen-Management kann das enorme Risiko für die informationstechnische Infrastruktur der Bundesrepublik hinnehmbar sein. In diesem Rahmen wäre ein Bündel von maßstabsbildenden Faktoren zu beachten, etwa

- die Verbreitung der Sicherheitslücke
  - in quantitativer Hinsicht: Zahl der betroffenen Nutzerinnen und Nutzer,
  - in qualitativer Hinsicht: Art der betroffenen Nutzerinnen und Nutzer,
- das Gewicht der Sicherheitslücke
  - zur Ausnutzung erforderlicher Aufwand,
  - aus der Ausnutzung resultierender Schaden,
- die Wahrscheinlichkeit, dass Betroffene die Ausnutzung der Lücke bemerken und im Einzelfall Gegenmaßnahmen einleiten,
- die Wahrscheinlichkeit einer technischen Lösung für die Lücke,
- die Wahrscheinlichkeit einer Verbreitung der technischen Lösung,
- Möglichkeiten zur Linderung der Folgen bei einer (zeitweisen) Geheimhaltung der Lücke,
  - die Wahrscheinlichkeit, dass Dritte die Lücke finden.

vgl. Herpig, Schwachstellen-Management für mehr Sicherheit, 2018, abrufbar unter https://www.stiftung-nv.de/sites/default/files/vorschlag.schwachstellenmanagement.pdf, zuletzt abgerufen am 01.07.2019.

Da §§ 15b, 15c HSOG kein ausdrückliches Verbot einer Nutzung und Geheimhaltung von Zero-Days zum Zweck der Infiltration enthalten und auch keine Vorgaben für ein behördliches Schwachstellen-Management errichten, sind die Vorschriften in diesem Punkt verfassungswidrig und bedürfen einer Ergänzung.

c) Anwendbarkeit auf juristische Personen

Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität von informationstechnischen Systemen gilt, soweit es sich auf Art. 2 Abs. 1 GG stützt, auch für inländische juristische Personen und damit auch für die Beschwerdeführerin zu 7. Denn es ist seinem Wesen nach auf juristische Personen anwendbar (Art. 19 Abs. 3 GG). Insoweit lässt sich die Rechtsprechung zum allgemeinen Persönlichkeitsrecht von juristischen Personen übertragen,

> BVerfGE 118, 168 (203), BGHZ 78, 24 (25).

Auch für juristische Personen besteht ein besonderes Schutzbedürfnis hinsichtlich des Schutzes ihrer IT-Systeme. Dies kann sich darauf gründen, dass innerhalb eines IT-Systems gespeicherte Daten weitreichende Rückschlüsse über die Arbeitsweise, Umsätze und Strategien der juristischen Person zulassen. Je nach Tätigkeit und Zweck der juristischen Person kann es sich aber auch gerade um eine IT-Infrastruktur handeln, deren Sicherheit neben der juristischen Person selbst noch zahlreiche weitere Nutzer*innen betrifft. Die Sicherheit dieses IT-Systems ist in diesen Fällen gewissermaßen die Kernaufgabe dieser juristischen Person. Das Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme knüpft damit an einem spezifischen Schutzbedürfnis an, welches auch juristische Personen betrifft und welches nicht von den übrigen Grundrechten abgedeckt wird. Insbesondere wird dies nicht von der informationellen Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) erfasst.

2. Anwendung zur automatisierten Datenanalyse, § 25a HSOG

a) Verfassungsrechtliche Maßstäbe

Die verfassungsrechtlichen Grenzen der automatisierten Datenanalyse mit Hilfe komplexer informationstechnischer Programme wurden in der Rechtsprechung des angerufenen Gerichts bislang nicht abschließend geklärt. Das angerufene Gericht hat in dem Urteil zum BKA-Gesetz zwischen zwei Weiterverarbeitungskonstellationen unterschieden, für die es unterschiedlich strenge verfassungsrechtliche Maßstäbe entwickelt hat. Eine Weiterverarbeitung erhobener Daten in einem Verfahren derselben Behörde im Rahmen derselben Aufgabe zum Schutz gleichwertiger Rechtsgüter wie im Ausgangsverfahren hält sich als weitere Nutzung im Rahmen der verfassungsrechtlichen Zweckbindung der Daten. Der Gesetzgeber darf eine solche weitere Nutzung unabhängig von weiteren gesetzlichen Voraussetzungen als bloßen Spurenansatz zulassen, der den Ausgangspunkt weiterer Ermittlungen bildet,

> vgl. BVerfGE 141, 220 (325 f.).

Hingegen ist eine Weiterverarbeitung durch eine andere Behörde oder durch dieselbe Behörde im Rahmen einer anderen Aufgabe als Zweckänderung besonders rechtfertigungsbedürftig. Der Gesetzgeber darf die zweckändernde Weiterverarbeitung nach dem Kriterium einer hypothetischen Datenneuerhebung zulassen, wenn der neue Verarbeitungszweck dem Erhebungszweck gleichwertig ist. In tatsächlicher Hinsicht setzt die Zweckänderung einen konkreten Ermittlungsansatz voraus,

vgl. BVerfGE 141, 220 (327 ff.).

Diese verfassungsrechtlichen Maßstäbe sind nicht ohne weiteres auf die spätere Analyse dieser Daten mit Hilfe einer komplexen Analysesoftware übertragbar. Die automatisierte Datenanalyse stellt keinen einfachen Fall der weiteren Nutzung dar, der lediglich den Anforderungen der Zweckbindung unterliegt.

Die Feststellung des angerufenen Gerichts im Urteil zum BKA-Gesetz, dass die Behörde gewonnene Kenntnisse zum Schutz derselben Rechtsgüter und im Rahmen derselben Aufgabenstellung - allein oder in Verbindung mit anderen ihr zur Verfügung stehenden Informationen - als schlichten Ausgangspunkt für weitere Ermittlungen nutzen kann,

vgl. BVerfGE 141, 220 (325),

hatten nicht die Generierung von Spurenansätzen mit Hilfe komplexer automatisierter Datenanalyseprogramme wie Hessendata zum Gegenstand. Diese Art der Datennutzung unterscheidet sich auch in wesentlichen Punkten von einer einfachen Weiternutzung.

Die herkömmliche Weiternutzung, wo einmal erhobene Daten, in einem zeitlichen Zusammenhang zum Erhebungsanlass, beispielsweise aufgrund eines Zufallsfundes, für neue Ermittlungen weitergenutzt werden, hat eine ganz andere Qualität als der automatisierte Zugriff auf alle verfügbaren Datenbestände. Bei Letzterem werden diese Daten gemeinsam in einem umfassenden Datenpool gespeichert und einer automatisierten Analyse unterzogen, um Ermittlungsansätze zu generieren. Im Unterschied zur herkömmlichen Weiternutzung erhobener Daten ermöglicht die Datenverknüpfung unter Einsatz komplexer Analyseprogramme die Erzeugung umfassender Sozialprofile verdächtiger Milieus und weitreichender Persönlichkeitsprofile von Einzelpersonen. Diese Art der Weiternutzung kann durch die ursprüngliche Datenerhebung nicht ohne Weiteres legitimiert werden.

Vor diesem Hintergrund ist die automatisierte Datenanalyse vielmehr an den im Urteil des angerufenen Gerichts entwickelten Maßstäben für die Rasterfahndung zu messen. Den Grundrechtseingriff, der durch die Rasterfahndung erfolgt, hat das angerufene Gericht als besonders intensiv bewertet. Zur Begründung wies das Gericht auf die Menge und Vielfalt der personenbezogenen Daten, die mit Hilfe von Informationstechnologie gegeneinander abgeglichen werden und dadurch in der Verarbeitung- und Verknüpfung einen neuen Stellenwert bekommen,

vgl. BVerfGE 115, 320 (350).

Wie bei der Anwendung zur automatisierten Datenanalyse, die über die unmittelbaren Zielpersonen auch eine fast unbegrenzte Zahl unbeteiligter Personen treffen kann, begründet auch die Rasterfahndung Eingriffsbefugnisse gegenüber Nichtstörern, um anhand der Daten einen

Verdacht zu generieren. Die große Menge der betroffenen Menschen, die für den Eingriff keinen Anlass gegeben haben, wertete das angerufene Gericht als eingriffsintensivierend,

> vgl. BVerfGE 115, 320 (354 ff.).

Eine neue Qualität und erhöhte Eingriffsintensität sah das Gericht zudem in der Nutzung automatisierter, rechnergestützter Operationen zur Verarbeitung nahezu beliebig großer und komplexer Informationsbestände in großer Schnelligkeit, wodurch Ermittlungstätigkeiten mit einer bislang unbekannten Durchschlagskraft versehen würden,

> BVerfGE 115, 320 (357).

Das angerufene Gericht ging in dieser Entscheidung noch weiter und beschrieb diese Form der Datenverarbeitung als Annäherung an die verfassungsrechtlich verbotene Erstellung umfassender Persönlichkeitsprofile,

> vgl. BVerfGE 115, 320 (351).

Schon im Volkszählungsurteil ging das angerufene Gericht auf die Möglichkeiten der Datenverknüpfung ein und sah die Gefahr eines Persönlichkeitsabbilds, wenn neu erhobene Daten mit den bei den Verwaltungsbehörden vorhandenen Daten verknüpft werden oder Lebens- und Personaldaten in einem Datenverbund erschlossen werden,

> „Das Erhebungsprogramm vermag zwar einzelne Lebensbereiche, zum Beispiel den Wohnbereich des Bürgers, jedoch nicht dessen Persönlichkeit abzubilden. Etwas anderes würde nur gelten, soweit eine unbeschränkte Verknüpfung der erhobenen Daten mit den bei den Verwaltungsbehörden vorhandenen, zum Teil sehr sensitiven Datenbeständen oder gar die Erschließung eines derartigen Datenverbundes durch ein einheitliches Personenkennzeichen oder sonstiges Ordnungsmerkmal möglich wäre“, BVerfGE 65, 1 (53).

Auch in jüngeren Jahren hat das angerufene Gericht bestätigt, dass es mit der Menschenwürde unvereinbar ist, „wenn eine hoheitliche Überwachung sich über einen längeren Zeitraum erstreckt und derart umfassend ist, dass nahezu alle Bewegungen und Lebensäußerungen des Betroffenen registriert werden und zur Grundlage für ein Persönlichkeitsprofil werden können […]“,

> BVerfGE 141, 220 (280).

Im Urteil zur Rasterfahndung etabliert das angerufene Gericht dementsprechend für Eingriffe, die der Erstellung umfassender Persönlichkeitsbilder nahekommen, hohe Eingriffsschwellen. Ein solcher Eingriff ist danach nur dann angemessen, wenn er an eine hinreichend konkrete Gefahr für hochrangige Verfassungsgüter anknüpft,

> vgl. BVerfGE 115, 320 (362).

b) Grundrechtswidrigkeit der automatisierten Anwendung zur Datenanalyse nach § 25a HSOG

Aufgrund der Möglichkeit, über Zielpersonen umfassende Persönlichkeitsbilder zu erzeugen, sowie der Streubreite in Bezug auf weitestgehend unbeteiligte Personen, weist die automatisierte Anwendung zur Datenanalyse eine hohe Eingriffsintensität auf (dazu unter (1)).

Gemessen an der Eingriffsintensität ist die Eingriffsermächtigung unverhältnismäßig, insbesondere ist sie hinsichtlich der Gefahrenschwelle und der geschützten Rechtsgüter zu weit (dazu unter (2)).

Zudem fehlt es an den erforderlichen Verfahrenssicherungen (dazu unter (3)).

(1) Intensität des Eingriffs

Die automatisierte Analyse gemäß § 25a HSOG stellt einen eigenen, besonders intensiven Eingriff in das Grundrecht auf informationelle Selbstbestimmung der Beschwerdeführer*innen zu 1-5 dar. Soweit personenbezogene Daten aus der Wohnraum- oder Telekommunikationsüberwachung in die Analyse einfließen, sind auch das Grundrecht auf Unverletzlichkeit der Wohnung aus Art. 13 Abs. 1 GG und das Fernmeldegeheimnis aus Art. 10 Abs. 1 GG betroffen. Der Grundrechtseingriff wiegt in Bezug auf die Zielpersonen und ihr unmittelbares Umfeld besonders schwer, weil die komplexe Verarbeitung großer Mengen an Daten die Erstellung umfassender Persönlichkeitsprofile ermöglicht (unter (i)). Für die zahlreichen Drittbetroffenen wiegt der Eingriff schwer, weil ihre personenbezogenen Daten ausgewertet werden, ohne dass sie dazu einen Anlass geboten haben (unter ii)).

Die automatisierte Datenanalyse ermöglicht durch die Kombination von Daten aus unterschiedlichen Quellen und die komplexe Verarbeitungstechnologie die Erzeugung nahezu umfassender Persönlichkeitsbilder und Sozialprofile verdächtiger Zielpersonen. Je größer die zugrundeliegenden Datenmengen sind und je leichter verknüpfbar, desto umfassender sind die Einblicke in die private Lebensführung der Betroffenen. Durch die komplexen softwarebasierten Verarbeitungs- und Verknüpfungsmöglichkeiten gewinnen zuvor möglicherweise belanglose Informationen einen neuen Gehalt,

> vgl. BVerfGE 115, 320 (350) „Die der Informationstechnologie eigenen Verarbeitungs- und Verknüpfungsmöglichkeiten, durch welche auch ein für sich gesehen belangloses Datum einen neuen Stellenwert bekommen".

§ 25a HSOG sieht keine Begrenzung des Umfangs der erfassten Daten vor. Eine solche ergibt sich auch mittelbar weder aus einer Begrenzung der Art der erfassten Daten noch aus einer Begrenzung des Adressatenkreises. Vielmehr können alle bei der Polizei Hessen erfassten Datenbestände genutzt werden und bei Bedarf auf Grundlage bestehender Ermächtigungsgrundlagen weitere erforderliche Daten bei externen öffentlichen wie privaten Stellen generiert werden. Hessendata speichert unter anderem die repressiven Daten aus polizeilichen Ermittlungsverfahren, präventive Daten, die zur Gefahrenabwehr erhoben wurden, alle Verkehrsdaten aus der Telekommunikationsüberwachung, sowie die von den Telekommunikationsanbietern zur Verfügung gestellten Daten. Zudem fließen auch externe Quellen ein, konkret genannt wurden im Untersuchungsausschuss zur Vergabe an das US-Unternehmen Palantir Informationen aus sozialen Netzwerken,

vgl. Zwischenbericht des Untersuchungsausschusses 19/3 zu Drucksache 19/6574 vom 03. Januar 2019, Seite 17.

Potenziell können in die automatische Datenanalyse jedoch alle Daten einfließen, die die Polizei legal erheben oder sich von anderen öffentlichen Stellen oder privaten Unternehmen übermitteln lassen kann. Nach § 13 HSOG hat die Polizei Hessen weitreichende Datenerhebungsbefugnisse und kann sich im Rahmen ihrer Aufgaben Daten von öffentlichen und privaten Stellen übermitteln lassen. Beispielsweise kann sich die Polizei nach §§ 13 HSOG, 22 HDSIG Daten zur Zielperson vom Landesamt für Verfassungsschutz, der Ausländerbehörde, der Meldebehörde, den Sozialämtern und weiteren öffentlichen Stellen übermitteln lassen, wenn dies zur Erfüllung ihrer Aufgaben erforderlich ist. Von privaten Stellen wie Banken, Verkehrsunternehmen oder Telekommunikationsanbietern kann sich die Polizei Kreditkarteninformationen, Reiserouten oder Verkehrs- und Verbindungsdaten übermitteln lassen.

Das Gewicht des Eingriffs verstärkt sich, wenn die einbezogenen Daten eine besondere Persönlichkeitsrelevanz aufweisen, für sich und in Verknüpfung mit anderen Daten. Besonders hoch ist die Eingriffsintensität, „wenn Informationen betroffen sind, bei deren Erlangung Vertraulichkeitserwartungen verletzt werden, vor allem solche, die unter besonderem Grundrechtsschutz stehen, wie etwa bei Eingriffen in das Grundrecht auf Unverletzlichkeit der Wohnung nach Art. 13 GG oder das Fernmeldegeheimnis nach Art. 10 GG“,

BVerfGE 115, 320 (348).

In den Polizeidatenbanken, die bei Hessendata einfließen, befinden sich auch ebensolche persönlichkeitsrelevanten Daten aus der Wohnraumüberwachung und der Telekommunikationsüberwachung.

In Bezug auf die jeweiligen Zielpersonen der polizeilichen Analyse kann die Kombination aus Daten aus der Telekommunikationsüberwachung und anderer Überwachungsmaßnahmen, beispielsweise Daten aus dem Melderegister, der Ausländerbehörde, dem Sozialamt oder Auskünfte von Verkehrsunternehmen oder Banken, kombiniert mit verfügbaren Informationen aus dem Internet teilweise schon nahezu lückenlose Einblicke in die Persönlichkeit und private Lebensführung dieser Personen bieten.

Angesichts der Menge und Vielfalt der personenbezogenen Daten, die heute über nahezu jede Person vorhanden sind und theoretisch im Wege der automatisierten Analyse ausgewertet werden können, nähert sich die automatisierte Datenanalyse jedenfalls bezüglich der Zielpersonen der von der Verfassung nicht zugelassenen Möglichkeit an, dass Daten mit anderen Datensammlungen zu einem teilweise oder weitgehend vollständigen Persönlichkeitsbild zusammengefügt werden,

vgl. zur Rasterfahndung die entsprechende Einschätzung des angerufenen Gerichts, BVerfGE 115, 320 (350 f.).

Der Umfang und die Vielfalt der potenziell analysierbaren Daten ist bei der automatisierten Datenanalyse nach § 25a HSOG noch höher als bei der Rasterfahndung, zudem sind hochsensible Daten aus der Wohnraumüberwachung und der Telekommunikationsüberwachung erfasst. Auch sind die Analysemöglichkeiten weitaus umfassender als bei der Rasterfahndung,

die sich auf zuvor festgelegte Suchkriterien beschränkt. Die automatisierte Datenanalyse hingegen stellt gemäß § 25a Abs. 2 HSOG Beziehungen oder Zusammenhänge zwischen Personen, Personengruppierungen, Institutionen, Organisationen, Objekten und Sachen her und ordnet die eingehenden Erkenntnisse bekannten Sachverhalten zu.

Auf die Intensität des Eingriffs wirken sich zudem daraus resultierende mögliche Folgemaßnahmen aus. Im Rasterfahndungsurteil wies das angerufene Gericht auf das Risiko für Betroffene hin, Gegenstand staatlicher Ermittlungsmaßnahmen zu werden,

> BVerfGE 115, 320 (351).

Ähnlich wie bei der Rasterfahndung begründet auch die automatisierte Anwendung zur Datenanalyse für betroffene Personen ein erhöhtes Risiko, Ziel weiterer behördlicher Ermittlungsmaßnahmen zu werden. Ergibt sich aus einer mit Hilfe der Datenanalyse generierten Hypothese ein Ermittlungsansatz, führt dies zu weiteren Ermittlungsmaßnahmen, sei es offenen Charakters wie Befragungen oder verdeckten Charakters wie Observationen oder Telekommunikationsüberwachung.

(i) Große Streubreite der Datenanalyse

Die Intensität des Eingriffs in die informationelle Selbstbestimmung begründet sich auch durch die große Streubreite der automatisierten Datenanalyse. Maßnahmen, bei denen zahlreiche Personen in den Wirkungsbereich einbezogen werden, die den Eingriff durch ihr Verhalten nicht veranlasst haben, sind grundsätzlich von hoher Eingriffsintensität,

> vgl. BVerfGE 100, 313 (376, 392); BVerfGE 115, 320 (347, 353); BVerfGE 120, 378 (402).

So liegt es hier: Von der automatisierten Datenanalyse ist keineswegs nur die jeweilige Zielperson betroffen, sondern zwangsläufig auch eine große Zahl von Menschen, die dafür keinen Anlass gegeben haben. Schließlich soll die Analyse Erkenntnisse über „gemeinsame Strukturen, Handlungsmuster, Personengruppen und zeitliche, sachliche, organisatorische, personale und situative Zusammenhänge“ bringen.

> LT- Drs. 19/6502, Seite 41.

Mithin bezieht die Analyse auch Daten von Menschen aus dem Umfeld der Zielperson und darüber hinaus auch von vollkommen unbeteiligten Menschen ein, die beispielsweise mit einem Ort oder einem Ereignis in Verbindung stehen. Schließlich kann jede Beziehung eines Objekts mit einem anderen Objekt zur Auswertung herangezogen werden und dies führt zu weiteren Objekten, die wieder mit anderen Objekten in Beziehung stehen. Diese Form der Analyse kann buchstäblich jeden treffen, bei Berücksichtigung von Melderegistern oder Fahrzeughalterdaten auch Menschen, die noch nie anlassbezogen polizeilich erfasst wurden. Auch dann, wenn die Datenerfassung letztlich nur der Verkleinerung der Treffermenge dient, kann in der Datenerhebung bereits ein Eingriff liegen, solange diese Daten nicht unmittelbar nach der Erfassung technisch anonym, spurenlos und ohne Erkenntnisinteresse für die Behörden ausgesondert werden,

> BVerfGE 115, 320 (343).

Die Herausforderung des Anwenders besteht darin, nur solche Objekte bzw. Beziehungen bei der Auswertung zu berücksichtigen, die tatsächlich relevant sind. Welche das sind, erkennt dieser allerdings erst bei der näheren Betrachtung,

> anschaulich macht dies ein Artikel der Frankfurter Rundschau, der am 02.07.2018 nach der Vorstellung von hessenDATA durch die Frankfurter Polizei erschien. „Projektleiter Bodo Koch“ [demonstrierte] „wie die Software den Ermittlern Netzwerke von Personen anzeigt, die etwa vom Handy eines Verdächtigen angerufen wurden oder in der Nähe einer beobachteten Wohnung leben. Auch Polizeifotos der Menschen aus dem Umfeld sind abrufbar“. Pitt v. Bebenburg: Beuth verteidigt Analysesoftware der Polizei, online abrufbar unter https://www.fr.de/rhein-main/spd-org26325/beuth-verteidigt-analysesoftware-polizei-11034270.html, zuletzt abgerufen am 01.07.2019

In manchen Fällen können durch die Analysesoftware generierte Verdachtsmomente gegenüber Drittbetroffenen vermutlich erst durch weitere, datenintensive Analysen oder gar durch weitere Folgemaßnahmen wie Telefonüberwachung oder Observation ausgeräumt werden.

(2) Eingriffsschwelle nicht hinreichend qualifiziert

Gemessen an der Intensität des Eingriffs genügt die Eingriffsermächtigung nicht dem Grundsatz der Verhältnismäßigkeit. Erstens fehlt es in Bezug auf die vorbeugende Straftatenbekämpfung in §25a Abs.1 HSOG an der erforderlichen konkreten Gefahr für gewichtige Rechtsgüter (i) und zweitens sind die in § 25a Abs. 1 HSOG normierten Rechtsgüter der Sachen von bedeutendem Wert und der gleichgewichtigen Umweltschäden zu unbestimmt (ii).

(i) Im Vorfeld einer konkreten Gefahr

Die vorbeugende Bekämpfung von in § 100a StPO genannten Straftaten ermöglicht den Einsatz der Datenanalyse weit im Vorfeld einer konkreten Gefahr. Insbesondere der unscharfe Begriff vorbeugenden Bekämpfung von Straftaten gewährleistet nicht, dass die Datenübermittlung an eine konkrete Gefahr im verfassungsrechtlichen Sinne gebunden wird, wie dies geboten ist.

Der Grundsatz der Verhältnismäßigkeit führt dazu, dass der Gesetzgeber intensive Grundrechtseingriffe erst von bestimmten Verdachts- oder Gefahrenstufen an vorsehen darf,

> vgl. BVerfGE 100, 313 (383f.); 109, 279 (350ff.).

Verzichtet der Gesetzgeber auf begrenzende Anforderungen an die Wahrscheinlichkeit des Gefahreneintritts sowie an die Nähe der Betroffenen zur abzuwehrenden Bedrohung und sieht er gleichwohl eine Befugnis zu Eingriffen von erheblichem Gewicht vor, genügt dies dem Verfassungsrecht nicht,

> BVerfGE 115, 320 (362).

Aufgrund des intensiven Persönlichkeitsbezugs und der hohen Streubreite des Grundrechtseingriffs verlangt das angerufene Gericht für die Rasterfahndung eine konkrete Gefahr für hochrangige Rechtsgüter,

> vgl. BVerfGE 115, 320 (362).

Auch die automatisierte Datenanalyse erfordert angesichts der hohen Eingriffsintensität eine konkrete Gefahr für hochrangige Rechtsgüter, dem genügt die vorbeugende Straftatenbekämpfung von in § 100a Abs. 2 StPO genannten Straftaten nicht.

Erstens knüpft der Eingriffstatbestand nicht an die gegenwärtige Begehung einer Straftat an, die zumindest in der Regel auf eine Rechtsgutsgefahr schließen lässt. Vielmehr wird der äußerst unbestimmte Begriff der vorbeugenden Bekämpfung genutzt. Danach bedarf es keiner tatsächlichen Anhaltspunkte für die bevorstehende Begehung einer Straftat, sondern es reichen im Zweifel abstrakte Gefahrenlagen. Dieses Begriffsverständnis deckt sich mit weiten Teilen der Gesetzgebungspraxis, Rechtsprechung und Literatur zum Polizeirecht,

> vgl. nur Denninger, in: Lisken/ders. (Hrsg.), Handbuch des Polizeirechts, 5. Aufl. 2012, Rn. D 1 ff., m.w.N.

Dieses Verständnis tritt auch in der Gesetzesbegründung zutage, wonach die Datenanalyse überhaupt erst der Gewinnung wesentlicher Anhaltspunkte für Gefahren und bevorstehende Straftaten dient,

> „Hierdurch könnten jedoch wesentliche Anhaltspunkte für Gefahren und bevorstehende Straftaten gewonnen werden, die mit der aktuellen IT-Struktur der Polizei unerkannt bleiben“, Hessischer Landtag, Drs. 19/6502, Seite 41.

Auf welcher Grundlage der Einsatz der automatisierten Datenanalyse fußen könnte, bleibt offen. Fast zwangsläufig wird es sich hierbei vor allem um vage und wenig aussagekräftige Faktoren wie die persönlichen Überzeugungen und sozialen Beziehungen des Betroffenen handeln, die für eine verfassungsrechtlich tragfähige Schadensprognose jedoch nicht ausreichen,

> „Eine Anknüpfung der Einschreitschwelle an das Vorfeldstadium ist verfassungsrechtlich angesichts der Schwere des Eingriffs nicht hinnehmbar, wenn nur relativ diffuse Anhaltspunkte für mögliche Gefahren bestehen. Die Tatsachenlage ist dann häufig durch eine hohe Ambivalenz der Bedeutung einzelner Beobachtungen gekennzeichnet. Die Geschehnisse können in harmlosen Zusammenhängen verbleiben, aber auch den Beginn eines Vorgangs bilden, der in eine Gefahr mündet“, BVerfGE 141, 220 (273).

Zweitens enthält der Straftatkatalog des § 100a Abs. 2 StPO auch Straftaten, deren Schutzgüter keineswegs äquivalent zu den in § 25a HSOG genannten Schutzgütern sind. Zu nennen sind mindestens das Verbreiten von Propagandamitteln verfassungswidriger Organisationen (§ 86 StGB), Geldfälschung (§146 Abs.1 StGB), Vorteilsgewährung (§333 Abs. 1 StGB), Verleitung zur missbräuchlichen Asylantragsstellung (§ 84 AsylG). § 100a StPO begrenzt den Anwendungsbereich der Telekommunikationsüberwachung über den Straftatenkatalog hinaus

im Abs. 1 auf Straftaten, die auch im Einzelfall schwer wiegen. Durch den unmittelbaren Verweis des § 25a Abs. 1 HSOG auf den Straftatenkatalog des § 100a Abs. 2 StPO fehlt diese Begrenzung.

Drittens enthält § 100a Abs. 2 StPO strafrechtliche Vorfeldtatbestände, deren bevorstehende Verwirklichung nicht zwingend auf eine konkrete Gefahr für ein besonders bedeutsames Rechtsgut schließen lässt. Im Straftatkatalog des § 100a StPO finden sich neben Erfolgsdelikten auch Gefährdungstatbestände, die Handlungen im Vorfeld einer Rechtsgutsverletzung kriminalisieren. Teilweise verlagern diese Tatbestände die Strafbarkeit erheblich vor. Beispielhaft sei auf § 129a StGB verwiesen, der bereits die Gründung oder Beteiligung an einer terroristischen Vereinigung bei Strafe verbietet, also eine Tathandlung weit im Vorfeld konkreter Schädigungshandlungen beschreibt. Eine sehr weitreichende Vorverlagerung der Strafbarkeit sieht auch § 89a StGB vor. Diese Norm stellt die Vorbereitung eines terroristischen Anschlags bereits in einem sehr frühen Stadium unter Strafe, wenn noch kaum absehbar ist, ob der Täter sein Vorhaben letztlich in die Tat umsetzen können wird. Die Rechtsprechung begrenzt die sehr weit gefasste Norm vor allem, indem sie hohe Anforderungen an den subjektiven Tatbestand stellt,

> vgl. BGH, Urteil vom 8. Mai 2014 – 3 StR 243/13 –, juris, Rn. 45; BGH, Urteil vom 27. Oktober 2015 – 3 StR 218/15 –, juris, Rn. 10.

Diese Begrenzung wirkt sich jedoch im präventiven Handlungsfeld allenfalls schwach aus. Denn im Voraus lassen sich die genauen Absichten und die Motivation des Betroffenen kaum erschließen. Eine präventiv ausgerichtete Überwachung muss darum ganz überwiegend an äußerliche, klar erkennbare Tatsachen anknüpfen. Vorfeldtatbestände wie § 129a oder § 89a StGB, die auf der objektiven Seite sehr weit gefasst sind, bieten deshalb kaum Anknüpfungspunkte, um die von § 25a HSOG geforderte Prognoseentscheidung normativ anzuleiten. Diese Entscheidung kann vielmehr in weitem Umfang an hoch ambivalente und vage Erkenntnisse anknüpfen.

(ii) Rechtsgüter zu unbestimmt

Ein Eingriff dieser Intensität ist mit der Verfassung nur vereinbar, wenn er dem Schutz oder der Bewahrung von hinreichend gewichtigen Rechtsgütern dient, für deren Gefährdung oder Verletzung im Einzelfall belastbare tatsächliche Anhaltspunkte bestehen. Die Einbeziehung von Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist, bedarf zumindest einer verfassungskonformen Auslegung, der Begriff der gleichgewichtigen Schäden für die Umwelt ist zu unbestimmt und daher genügt den verfassungsrechtlichen Anforderungen an das Gewicht des geschützten Rechtsguts nicht.

Im Urteil zur Vorratsdatenspeicherung sowie im Urteil zur Rasterfahndung sah das angerufene Gericht den Abruf der betroffenen Daten nur zur Abwehr einer Gefahr für Leib, Leben oder Freiheit einer Person, für den Bestand oder die Sicherheit des Bundes oder eines Landes als zulässig an,

> vgl. BVerfGE 125, 260 (330); BVerfGE 115, 320 (357).

Für die Datenerhebung im Wege verdeckter Überwachungsmaßnahmen hat das angerufene Gericht „[e]inen uneingeschränkten Sachwertschutz“ insoweit „nicht als ausreichend gewichtig [...] angesehen“,

> BVerfGE 141, 220 (270).

Das angerufene Gericht hat daher festgehalten, dass mit Blick auf den Einsatz besonderer Mittel der Datenerhebung nach § 20g Abs. 1 BKAG a.F. das dortige Merkmal des Schutzes von „Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist“ bei „verständiger Auslegung“ eng zu verstehen sei und – (nur) so verstanden – die Überwachungsmaßnahmen auf den Schutz hinreichend gewichtiger Rechtsgüter begrenze:

> „Bei verständiger Auslegung kann hierunter nicht schon allein der Schutz von bedeutsamen Sachwerten verstanden werden. Gemeint sind hier im gesetzlichen Zusammenhang mit der Terrorismusabwehr vielmehr etwa wesentliche Infrastruktureinrichtungen oder sonstige Anlagen mit unmittelbarer Bedeutung für das Gemeinwesen [...].“, BVerfGE 141, 220 (287).

Im Urteil zur Vorratsdatenspeicherung sowie im Urteil zur Rasterfahndung sah das angerufene Gericht den Abruf der betroffenen Daten nur zur Abwehr einer Gefahr für Leib, Leben oder Freiheit einer Person, für den Bestand oder die Sicherheit des Bundes oder eines Landes als zulässig an,

> vgl. BVerfGE 125, 260 (330); BVerfGE 115, 320 (357).

Eine Sache von bedeutendem Wert im Sinne des § 315b Abs. 1 StGB ist nach ständiger Rechtsprechung des BGH schon ab einem Wert von EUR 750 zu bejahen,

> vgl. BGH, Urteil vom 4. Dezember 2002 – 4 StR 103/02, BGHSt, 48, 119; Beschluss vom 20. Oktober 2009 – 4 StR 408/09.

Im öffentlichen Interesse können bereits eine öffentliche Sitzbank oder andere im Visier von Sprühern stehende Gegenstände liegen, so dass eine automatisierte Datenanalyse zur Durchleuchtung der Sprüherszene ermöglicht wäre. Angesichts der Intensität der Datenanalyse sind die in § 25a Abs. 1 HSOG normierten Sachen von bedeutendem Wert, deren Erhalt im öffentlichen Interesse liegt, zumindest im Sinne des Urteils zum BKA-Gesetz so auszulegen, dass nur wesentliche Infrastruktureinrichtungen oder sonstige Anlagen mit unmittelbarer Bedeutung für das Gemeinwesen gemeint sind.

Auch der Begriff des gleichgewichtigen Schadens an der Umwelt ist zu unbestimmt. Der Erhalt der Umwelt liegt grundsätzlich im öffentlichen Interesse, zudem führen Umweltverschmutzungen weit überwiegend zu erheblichen Schadenssummen, die weit über EUR 750 liegen. Man denke nur an die alltäglichen und doch gewichtigen Umweltschäden, die durch den Straßenverkehr, den Pestizideinsatz oder den Flugverkehr entstehen. Vor diesem Hintergrund ist das Rechtsgut zu präzisieren oder stattdessen auf konkrete Umweltstraftatbestände zu verweisen.

Der Unbestimmtheit der Rechtsgüter vermag auch nicht abzuhelfen, dass bei gebotener Berücksichtigung des Zweckbindungsgrundsatzes gemäß § 20 HSOG die Daten aus besonders

schweren Grundrechtseingriffen (wie beispielsweise der Wohnraumüberwachung) nicht für eine Datenanalyse zum Schutz von bedeutsamen Sachwerten oder der Umwelt herangezogen werden können. Schließlich sind auch in den nutzbaren Datenbeständen große Datenmengen vorhanden, die bei Verknüpfung neue, weitreichende Erkenntnisse über die Zielperson zutage fördern können.

(3) Verfahrenssicherungen

Bei der Speicherung und Nutzung personenbezogener Daten für die behördliche Aufgabenwahrnehmung hat der Gesetzgeber unter Verhältnismäßigkeitsgesichtspunkten auch Anforderungen an Transparenz, Rechtsschutz und Kontrolle zu beachten,

BVerfGE 133, 277 (366).

§ 25a HSOG erfüllt keine dieser Anforderungen und verletzt damit nicht nur das Grundrecht der Beschwerdeführer*innen auf informationelle Selbstbestimmung aus Art. 1 Abs. 1 GG i.V. mit Art. 2 Abs. 1 GG, sondern auch das Grundrecht auf individuellen Rechtsschutz nach Art. 19 Abs. 4 GG.

§ 25a HSOG enthält keinerlei transparenzschaffende Regelungen. Weder muss eine Zielperson über eine in Bezug auf sie durchgeführte automatisierte Datenanalyse nachträglich benachrichtigt werden, noch besteht nach § 25a HSOG ein Auskunftsrecht der betroffenen Personen.

Nach § 29 HSOG i.V. mit §§ 50-52 HDSIG existieren Benachrichtigungspflichten und Auskunftsrechte in Bezug auf die bei der Polizei Hessen gespeicherten personenbezogenen Daten einer Person. Davon umfasst ist jedoch nicht die Information über die Nutzung dieser Daten in Form einer automatisierten Datenanalyse gemäß § 25a HSOG.

Angesichts der Schwere des Eingriffs, der über die bereits vorhandenen personenbezogenen Daten einer Person weitergehende Erkenntnisse bis hin zu weitreichenden Persönlichkeitsbildern generieren kann, ist der Verzicht auf transparenzschaffende Vorgaben wie Auskunftsrechte und Benachrichtigungspflichten unverhältnismäßig.

Entsprechende Benachrichtigungspflichten und Auskunftsrechte würden auch nicht den Zweck der Maßnahme unterlaufen, wenn sie erst nach Abschluss einer Anwendung zur automatisierten Datenanalyse zur Anwendung kämen.

Auch in Bezug auf die Gewährleistung einer wirksamen Aufsicht verfehlt § 25a HSOG die verfassungsrechtlichen Anforderungen. Die Anordnung der Datenanalyse erfolgt nach § 25a Abs. 3 HSOG durch die Behördenleitung oder durch einer oder eines von dieser beauftragten Bediensteten. Zudem ist die oder der Datenschutzbeauftragte vor der Einrichtung oder wesentlichen Änderung anzuhören, bei Gefahr im Verzug ist die Anhörung nachzuholen. Im Wesentlichen kann jede beauftragte Person bei der Polizei die automatisierte Analyse anordnen, bei Gefahr auch ohne Anhörung der*s Datenschutzbeauftragten. Erfolgt eine Anhörung des*r Datenschutzbeauftragten, folgen hieraus keine zwingenden Konsequenzen. Zudem fehlen der*m Datenschutzbeauftragten die Zugriffsrechte auf die Datenanalyse, um die Reichweite im Einzelfall umfassend beurteilen zu können.

Die Schwere des Eingriffs erfordert einen Richtervorbehalt, zumindest jedoch die Zustimmung eines*r mit Zugriffsbefugnissen ausgestatteten Datenschutzbeauftragten. Weiterhin ist erforderlich, dass die jeweiligen Anwendungen zur automatisierten Datenanalyse vollständig protokolliert werden. Diese prozessualen Vorgaben müssen zur Wahrung der Verhältnismäßigkeit auch gesetzlich verankert sein.

Zudem fehlt es in § 25a HSOG an eingrenzenden Vorgaben zur Dauer der Maßnahme, zur Löschung der durch die automatisierte Datenanalyse generierten Erkenntnisse und zur Anwendung der aus den Grundsätzen der Zweckbindung und Zweckänderung resultierenden Beschränkungen nach § 20 HSOG.

Zwar mögen die allgemeinen Regelungen zur Löschung von Daten gemäß §§ 27, 28 HSOG, sowie zur Zweckbindung nach § 20 HSOG anwendbar sein, aufgrund der Besonderheiten der automatisierten Datenanalyse lassen diese Regelungen gleichwohl wesentliche Fragen unbeantwortet. Fraglich ist beispielweise, ob die Löschfristen nach § 20 Abs. 4 HSOG sich jeweils verlängern, wenn Daten innerhalb der automatisierten Datenanalyse generiert und diese Verknüpfungen dort gespeichert werden. Die Maßgaben der Zweckbindung nach § 20 Abs. 1 HSOG lassen sich nicht ohne Weiteres auf die automatisierte Datenanalyse übertragen, vielmehr bedarf es angesichts der Schwere des Eingriffs eines konkreten Ermittlungsanlasses,

vgl. unter D II 2 a.

Prof. Dr. Tobias Singelnstein